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

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. 欧几里得除法　不完全商　余数
5. 整数的 b- 进制表示
6. 最大公因数
7. 广义欧几里得除法
8. 整数的性质　最小公倍数
9. 算术基本定理
10. 素数定理

节考虑关于　　概念和　　和　　.

*** 定义 1** 设 a, b 是任意两个　　，其中 $b \neq 0.$　果存在一个 q 使　等式

$$a = bq \tag{1}$$

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

注 1　　仅与乘　运　相关, 与　学　　有极　区别.

注 2　　可推　为现代　学　　.

3 当 b 遍历 a 所 $-b$ 遍历 a 所

4 当 b 遍历 a 所 a/b 遍历 a 所

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

$2, 3, 5$ 分 30 30 $2, 3, 5$ 分 $2|30, 3|30, 5|30$. $2, 3, 5$ 都 30 30 $2, 3, 5$

30 所 $\{\pm 1, \pm 2, \pm 3, \pm 5, \pm 6, \pm 10, \pm 15, \pm 30\}$, $\{\mp 1, \mp 2, \mp 3, \mp 5, \mp 6, \mp 10, \mp 15, \mp 30\}$, $\{\pm 30 = 30/\pm 1, \pm 15 = 30/\pm 2, \pm 10 = 30/\pm 3, \pm 6 = 30/\pm 5, \pm 5 = 30/\pm 6, \pm 3 = 30/\pm 10, \pm 2 = 30/\pm 15, \pm 1 = 30/\pm 30\}$.

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

* 0 何非零 1 何 何非零 a 自身 自身

2 $a,\ b$ 若 $b|a,$ $b \mid (-a),\ (-b)|a,\ (-b)|(-a).$

证 $b|a,$ q $a = bq.$ 而

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

$-q,\ q$ 根据 $b \mid (-a),\ (-b)|a,\ (-b)|(-a).$

* **理 1** $a,\ b \neq 0,\ c \neq 0$ 若 $c|b,\ b|a,$ $c|a.$(**传递性**)

证 $c|b,\ b|a,$ 根据 $q_1,\ q_2$

$b = cq_1, \quad a = bq_2.$ 此 我们

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

$q = q_1q_2$ 以根据 $c|a.$

证明

* **3** $7|42,\ 42|84$, 以 $7|84.$

2 $a,\ b,\ c \neq 0$ $c|a,\ c|b,$ $c|a \pm b.$(**加法运算**)

$c|a,\ c|b,$ 那么 $q_1,\ q_2$ $a = cq_1, \quad b = cq_2.$

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

$q_1 \pm q_2$ $a \pm b$ c

4 $7|14,\ 7|84,$ $7|(84 + 14) = 98, \quad 7|(84 - 14) = 70.$

***** **3** $a,\ b,\ c \neq 0$ $c|a,\ c|b,$ 对 $s,\ t,$ $c|sa + tb.$ (**系 线 组合**)

$c|a,\ c|b,$ 那么 $q_1,\ q_2$ $a = cq_1, \quad b = cq_2.$

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

$sq_1 + tq_2$ $sa + tb$ c

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

* **6** $a,\ b,\ c\neq 0$ 三 $c|a,\ c|b.$ $s,\ t,$

$sa+tb=1,\qquad c=\pm 1.$

$c|a,\ c|b,$ $s,\ t,$ $sa+tb=1,$ 3,

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

$c=\pm 1.$

3

4 $a_1,\ \ldots,\ a_n$ $c\neq 0$

n $s_1,\ \ldots,\ s_n,$

$$s_1a_1+\cdots+s_na_n$$

c

7 $7|14,\ 7|21,\ 7|35,$

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

* **5** $a,\ b$ $a|b,\ b|a,$ $a=\pm b.$

$a|b,\ b|a,$ $q_1,\ q_2$

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

从

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

样 $q_1q_2=1.$ $q_1,\ q_2$ $q_1=q_2=\pm 1.$

$a=\pm b.$

前面 了 继续 解

* **2** $n \neq 0, \pm 1$. 除了显然因数 ± 1 和 $\pm n$ 外, n 没

它 n **素** (或 **质数** 或 **不可约数**), n .

因 n 和 $-n$ 同为素数或合数, 总 指正 通 p.

8 $2, 3, 5, 7$; $4, 6, 10, 15, 21$

面 每 必 子

* **6** n 正 p n 1 正

p 且 $p \leq \sqrt{n}$.

反 p q, $1 < q < p$, $q|p$. 但 $p|n$,

由 1, $q|n$. p n 正 矛盾 p

n $n = pn_1, \quad 1 < p \leq n_1 < n.$ $p^2 \leq n$.

$p \leq \sqrt{n}$.

6, 即 到 判

* **7** $n > 1$. $p \le \sqrt{n}$, $p \not| n$, n

* 应用 7, 寻找 确 方

厄拉托塞师 (Eratosthenes) 筛 .

给 N , 求出 超过 N

列出 N 删 $\le \sqrt{N}$ $p_1, \ldots, p_k$

具体地 依次删

$$p_1 : \quad 2p_1, \ldots, [\frac{N}{p_1}]p_1;$$

$$\ldots\ldots$$

$$p_1 : \quad 2p_k, \ldots, [\frac{N}{p_k}]p_k,$$

(包括 1) 求 超过 N

9 $N = 100$

解 $\leq \sqrt{100} = 10$ $2,\ 3,\ 5,\ 7,$

$2,\ 3,\ 5,\ 7$

$$
\begin{array}{lllll}
2 \cdot 2, & 3 \cdot 2, & 4 \cdot 2, & \ldots, & 49 \cdot 2, \quad 50 \cdot 2 \\
2 \cdot 3, & 3 \cdot 3, & 4 \cdot 3, & \ldots, & 32 \cdot 3, \quad 33 \cdot 3 \\
2 \cdot 5, & 3 \cdot 5, & 4 \cdot 5, & \ldots, & 19 \cdot 5, \quad 20 \cdot 5 \\
2 \cdot 7, & 3 \cdot 7, & 4 \cdot 7, & \ldots, & 13 \cdot 7, \quad 14 \cdot 7.
\end{array}
$$

(1) $N = 100$

上 答

$p_1 = 2,$

1	2	3	$\not{4}$	5	$\not{6}$	7	$\not{8}$	9	$\not{10}$
11	$\not{12}$	13	$\not{14}$	15	$\not{16}$	17	$\not{18}$	19	$\not{20}$
21	$\not{22}$	23	$\not{24}$	25	$\not{26}$	27	$\not{28}$	29	$\not{30}$
31	$\not{32}$	33	$\not{34}$	35	$\not{36}$	37	$\not{38}$	39	$\not{40}$
41	$\not{42}$	43	$\not{44}$	45	$\not{46}$	47	$\not{48}$	49	$\not{50}$
51	$\not{52}$	53	$\not{54}$	55	$\not{56}$	57	$\not{58}$	59	$\not{60}$
61	$\not{62}$	63	$\not{64}$	65	$\not{66}$	67	$\not{68}$	69	$\not{70}$
71	$\not{72}$	73	$\not{74}$	75	$\not{76}$	77	$\not{78}$	79	$\not{80}$
81	$\not{82}$	83	$\not{84}$	85	$\not{86}$	87	$\not{88}$	89	$\not{90}$
91	$\not{92}$	93	$\not{94}$	95	$\not{96}$	97	$\not{98}$	99	$\not{100}$

$p_2 = 3,$

1	2	3	5	7	$\not{9}$
11		13	$\not{15}$	17	19
$\not{21}$		23	25	$\not{27}$	29
31		$\not{33}$	35	37	$\not{39}$
41		43	$\not{45}$	47	49
$\not{51}$		53	55	$\not{57}$	59
61		$\not{63}$	65	67	$\not{69}$
71		73	$\not{75}$	77	79
$\not{81}$		83	85	$\not{87}$	89
91		$\not{93}$	95	97	$\not{99}$

$p_3 = 5,$

1	2	3	5	7	
11		13		17	19
		23	$\not{2}5$		29
31			$\not{3}5$	37	
41		43		47	49
		53	$\not{5}5$		59
61			$\not{6}5$	67	
71		73		77	79
		83	$\not{8}5$		89
91			$\not{9}5$	97	

$p_4 = 7,$

1	2	3	5	7	
11		13		17	19
		23			29
31				37	
41		43		47	$\not{4}9$
		53			59
61				67	
71		73		$\not{7}7$	79
		83			89
$\not{9}1$				97	

(1) $N = 100$

~~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	

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.

* **8** 无穷多

假 只 限 $p_1,\ p_2,\ \ldots,\ p_k.$

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

$n > p_i, \quad i = 1, \ldots, k,$ n $6, n$

1 p p $p_1,\ p_2,\ \ldots,\ p_k$ 某

$j,\ 1 \le j \le k,$ $p = p_j.$ 3,

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

无穷多

形 $4k+3$ 无穷多 无

形 $4k+1$ 无穷多 需 更多技巧

之间 系 引 **欧几里得 (Euclid)** **带余** .

* **9** ( ) $a,\ b$ $b > 0.$

惟 $q,\ r$

$$a = bq + r, \quad 0 \le r < b \tag{2}$$

9 之 明: ( ) 序

$$\ldots,\ -3b,\ -2b,\ -b,\ 0,\ b,\ 2b,\ 3b,\ \ldots.$$

实 轴 长度 b 间 a 落

间 q $qb \le a < (q+1)b.$

令 $r = a - bq,$ $a = bq + r, \quad 0 \le r < b.$

( ) $q,\ r$ $q_1,\ r_1$ 满足 (2),

$$a = bq + r, \qquad 0 \le r < b,$$
$$a = bq_1 + r_1, \quad 0 \le r_1 < b.$$

减 $b(q - q_1) = -(r - r_1).$

$q \ne q_1$ 左边 绝 值 $\ge b,$ 右边 绝 值 $< b.$

$q = q_1, \quad r = r_1.$

* **3** (2) q a b **不完全商**, r

a b .

推论 9 条件 $b|a \Leftrightarrow r = 0.$

密码 起着核心 改

密码 统 效率 $b = 2^u + v$, v 很

7 断

10 $N = 137$

$\leq \sqrt{137} < 12$ $2,\ 3,\ 5,\ 7,\ 11,$

$2,\ 3,\ 5,\ 7,\ 11$ 去试

$$137 = 68 \cdot 2 + 1, \quad 137 = 45 \cdot 3 + 2, \quad 137 = 26 \cdot 5 + 3,$$
$$137 = 19 \cdot 7 + 4, \quad 137 = 12 \cdot 11 + 5.$$

$2 \not| 137,\ 3 \not| 137,\ 5 \not| 137,\ 7 \not| 137,\ 11 \not| 137.$ $7, N = 137$

好 描 及今后 些

符号

4 x x 部

x $[x]$.

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

9 q $q=[\frac{a}{b}]$, r $r=a-b[\frac{a}{b}]$.

事 先计 $q=[\frac{a}{b}]$, 再计 $r=a-b[\frac{a}{b}]$.

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

12 $b=15.$

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

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

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

际 取

10 ( ) $a,\ b$ $b > 0.$

c , $q,\ r$

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

1. $0 \le r < b$ r **最小非负** .
2. $1 \le r \le b$ r **最小正** .
3. $-b+1 \le r \le 0$ r **最大非正** .
4. $-b \le r < 0$ r **最大负** .
5. $-b/2 \le r < b/2$ $-b/2 < r \le b/2$ r **绝对值最小** .

13 $b = 7$.

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.

14 $b = 8$.

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.

平 遇 10 51328

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

中国是世界上最早采用十进制的国家，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：

1 $b > 1$ n

$$n = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \cdots + a_1 b + a_0,$$

a_i $0 \le a_i \le b-1,\ i = 1, \ldots, k-1,$ 首项 $a_{k-1} \neq 0.$

n 达 逐

b n $n = bq_0 + a_0, \quad 0 \le a_0 \le b-1.$

b q_0 $q_0 = bq_1 + a_1, \quad 0 \le a_1 \le b-1.$

$$\begin{aligned} q_1 &= bq_2 + a_2, \quad 0 \le a_2 \le b-1, \\ &\dots \\ q_{k-3} &= bq_{k-2} + a_{k-2}, \quad 0 \le a_{k-2} \le b-1, \\ q_{k-2} &= bq_{k-1} + a_{k-1}, \quad 0 \le a_{k-1} \le b-1. \end{aligned}$$

$0 \le q_{k-1} < \cdots < q_1 < q_0 < n,$ k

$q_{k-1} = 0.$

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

种　同

$$n = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \cdots + a_1 b + a_0, \quad 0 \le a_i \le b-1,\ i = 1, \ldots, k-1.$$

$$n = c_{k-1}b^{k-1} + c_{k-2}b^{k-2} + \cdots + c_1 b + c_0, \quad 0 \le c_i \le b-1,\ i = 1, \ldots, k-1. \ ($$

$$a_{k-1} = 0 \qquad c_{k-1} = 0.)$$

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

j $a_j \neq c_j,$

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

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

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

$b|(a_j - c_j), \quad |a_j - c_j| \ge b.$ $0 \le a_j \le b-1, \quad 0 \le c_j \le b-1,$

$|a_j - c_j| < b.$ 说 n

b

1 $n = (a_{k-1}a_{k-2}\ldots a_1a_0)_b$ 展开

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

$0 \le a_i \le b-1,\ i = 1, \ldots, k-1,\ a_{k-1} \neq 0,$ n b

进制表示. n b- 位 $k = [\log_b n] + 1.$

$b^{k-1} \le n < b^k$ $k - 1 \le \log_b n < k.$

$k - 1 = [\log_b n].$

1 642 2

$$
\begin{aligned}
642 &= 2\cdot 321 + 0, \\
321 &= 2\cdot 160 + 1, \\
160 &= 2\cdot 80 + 0, \\
80 &= 2\cdot 40 + 0, \\
40 &= 2\cdot 20 + 0,
\end{aligned}
\qquad
\begin{aligned}
20 &= 2\cdot 10 + 0, \\
10 &= 2\cdot 5 + 0, \\
5 &= 2\cdot 2 + 1, \\
2 &= 2\cdot 1 + 0, \\
1 &= 2\cdot 0 + 1.
\end{aligned}
$$

$$642 = (1010000010)_2\ ,$$

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

机 8 16 64 16

$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ A,\ B,\ C,\ D,\ E,\ F$

$0,\ 1,\ \ldots,\ 15$ 共 16 $A,\ B,\ C,\ D,\ E,\ F$

$10,\ 11,\ 12,\ 13,\ 14,\ 15.$

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	1	0011	11	B	1011
4	1	0100	12	C	1100
5	1	0101	13	D	1101
6	1	0110	14	E	1110
7	1	0111	15	F	1111

例 3 转换 16 进制 $(ABC8)_{16}$ 为 2 进制.

因 $A=(1010)_2, B=(1011)_2, C=(1100)_2, 8=(1000)_2$.

$$(ABC8)_{16}=(1010101111001000)_2.$$

4 转换 2 $(1011101111111101001)_2$ 16
换

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

$$(1011101111111101001)_2 = (5DFE9)_{16}.$$

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.

5 642 16

1, $642 = (1010000010)_2$.

查换

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

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

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.

1　$a_1,\ \ldots,\ a_n$　$n\ (n \geq 2)$　d

d　$a_1,\ \ldots,\ a_n$　**公**　.

$a_1,\ \ldots,\ a_n$　$a_1,\ \ldots,\ a_n$

公　，　$(a_1, \ldots, a_n)$. 特

$(a_1, \ldots, a_n) = 1$　$a_1,\ \ldots,\ a_n$ **互**　**互质**.

$d = (a_1,\ \ldots,\ a_n)$　叙

(1) $d|a_1,\ \ldots,\ d|a_n$.　(2)　$e|a_1,\ \ldots,\ e|a_n$,　$e|d$.

我们将在定理 7 中给予说明.

1　14　21　$\{\pm 1,\ \pm 7\}$,

$(14, 21) = 7$.

2 -15 21 $\{\pm 1,\ \pm 3\}$,
$(-15, 21) = 3$.

3 $14,\ -15$ 21 $\{\pm 1\}$,
$(14, -15, 21) = 1$. $14,\ -15$ 21 互

4 $a,\ b$ $(b,\ a) = (a,\ b)$.

5 $a,\ b$ $b|a,$ $(a,\ b) = b$.

6 p a $p \not| a,$ p a 互

$(p, a) = d$. $d|p$ $d|a$.

p $d|p,$ $d = 1$ $d = p$.

$d = p,$ $d|a,$ $p|a,$ $p \not| a$

$d = 1$. $(p, a) = 1$. 结论

1 $a_1,\ \ldots,\ a_n$ n

(i) $a_1,\ \ldots,\ a_n$ $|a_1|,\ \ldots,\ |a_n|$

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

7 $a,\ b$ $(a,\ b) = (a,\ -b) = (-a,\ b) = (|a|,\ |b|)$

8

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

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

***** **2** b $(0,b)=b.$

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 $(0,b)=b.$

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

***** **3** $a,\ b,\ c$ $a=bq+c,$

q $(a,b)=(b,c).$

$d=(a,b),\ d'=(b,c),$ $d|a,\ d|b.$ §1.1 3,

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

d $b,\ c$ $d\le d'.$

d' $a,\ b$ $d'\le d.$

$d=d'.$ 3

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

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

怎 才 $a,\ b$ ？直接

知道 $a,\ b$

行 见 §1.5 4. $a,\ b$

困难 “

辗 ”, 然 $a,\ b$

*** 广** $a,\ b$

$r_{-2} = a,\ r_{-1} = b.$ 复

$$
\begin{aligned}
r_{-2} &= q_0 r_{-1} + r_0, && 0 \le r_0 < r_{-1}, \\
r_{-1} &= q_1 r_0 + r_1, && 0 \le r_1 < r_0, \\
r_0 &= q_2 r_1 + r_2, && 0 \le r_2 < r_1, \\
&\cdots\cdots && \\
r_{n-4} &= q_{n-2} r_{n-3} + r_{n-2}, && 0 \le r_{n-1} < r_{n-2}, \\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1}, && 0 \le r_{n-1} < r_{n-2}, \\
r_{n-2} &= q_n r_{n-1} + r_n, && r_n = 0.
\end{aligned}
\tag{1}
$$

经过有限步骤，必然存在 n 使得 $r_n = 0$, 这是因为

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

且 b 是有限正整数.

4 $a,\ b$ $(a,b) = r_{n-1},$ r_{n-1}

(1)

3,

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

2,

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

$O(\log a \log b),$ $n\ =$

$O(\log a),$ (a,b) $O(\log^2 a \log b).$

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.

12 $a = -1859,\ b = 1573,$ (a, b).

1, $(-1859, 1573) = (1859, 1573)$.

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

4, $(-1859, 1573) = 143$.

14 $a = 46480,\ b = 39423,$ (a, b).

利 负

$$46480 = 1 \cdot 39423 + 7057 \qquad 1219 = 2 \cdot 481 + 257 \qquad 26 = 3 \cdot 7 + 5$$
$$39423 = 5 \cdot 7057 + 4138 \qquad 481 = 1 \cdot 257 + 224 \qquad 7 = 1 \cdot 5 + 2$$
$$7057 = 1 \cdot 4138 + 2919 \qquad 257 = 1 \cdot 224 + 33 \qquad 5 = 2 \cdot 2 + 1$$
$$4138 = 1 \cdot 2919 + 1219 \qquad 224 = 6 \cdot 33 + 26 \qquad 2 = 2 \cdot 1.$$
$$2919 = 2 \cdot 1219 + 481 \qquad 33 = 1 \cdot 26 + 7$$

方法二：绝对值最小余数.

$$46480 = 1 \cdot 39423 + 7057 \qquad 1219 = 3 \cdot 481 - 224 \qquad 7 = 3 \cdot 2 + 1$$
$$39423 = 6 \cdot 7057 - 2919 \qquad 481 = 2 \cdot 224 + 33 \qquad 2 = 2 \cdot 1.$$
$$7057 = 2 \cdot 2919 + 1219 \qquad 224 = 7 \cdot 33 - 7$$
$$2919 = 2 \cdot 1219 + 481 \qquad 33 = 5 \cdot 7 - 2$$

$$(46480,\ 39423) = 1.$$

从广义欧几里得除法的演示中，我们观察到

$$\begin{aligned} r_n &= r_{n-2} - r_{n-1}q_{n-1}, \\ r_{n-1} &= r_{n-3} - r_{n-2}q_{n-3}, \\ &\cdots\cdots \\ r_3 &= r_1 - r_2q_2, \\ r_2 &= r_0 - r_1q_1. \end{aligned}$$

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

15 $a=-1859,\ b=1573,$ $s,\ t$, $sa+tb=(a,b)$.

12 ,

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

$s=5,\ t=6$ $sa+tb=(a,b)$.

17 $a = 46480,\ b = 39423,$ $s,\ t\ ,$ $sa + tb = (a, b).$

解 由例 14 , 我们有方法一：最小非负余数.

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

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

$$
s=-22703,\ t=26767 \qquad\qquad sa+tb=(a,b).
$$

* **5** $a,\ b$ $s_n a + t_n b = (a, b), \quad (2)$

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

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

q_j (1)

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

r_j (1) $(a, b) = r_n,$

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

j 归纳 来 (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.

$$1 \leq j \leq k-1$$

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

$j = k$,

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

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

$j = k$ 原 (4)

j

$a,\ b$ $s,\ t$

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

$$r_{-2} = a,\ r_{-1} = b, \quad s_{-2} = 1,\ s_{-1} = 0, \quad t_{-2} = 0,\ t_{-1} = 1.$$

(1) $r_{-1} = 0, \qquad s = s_{-2}, \quad t = t_{-2}.$

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

(2) $r_0 = 0, \qquad s = s_{-1}, \quad t = t_{-1}.$

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

(3) $r_1 = 0, \qquad s = s_0, \quad t = t_0.$

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

.....

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

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

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

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

$$r_n = 0.$$

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

$$s,\ t,$$

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

程　　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
⋮	⋮	⋮	⋮	⋮
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

$$\begin{cases} s_{j-1} = s_{j-3} - q_{j-1}s_{j-2}, \\ t_{j-1} = t_{j-3} - q_{j-1}t_{j-2}, \\ q_j = [\dfrac{r_{j-2}}{r_{j-1}}], \\ r_j = r_{j-2} - q_j r_{j-1}. \end{cases}$$

18 $a = 1859,\ b = 1573.$ $s,\ t$

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

(5) (6),

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

$s = -5,\ t = 6$

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

19 $a = 737,\ b = 635.$ $s,\ t$

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

(5) (6),

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

$s = 193,\ t = -224$

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

5 逆命

* **6** $a,\ b$ 充 $s,\ t$

$$sa + tb = 1.$$

5, 命

$d = (a, b),$ $d|a,\ d|b.$ $s,\ t$

$$sa + tb = 1.$$

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

$d = 1.$ $a,\ b$

20 四 $a,\ b,\ c,\ d$

$$ad - bc = 1.$$

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

***** **7** $a,\ b$ d

d $a,\ b$

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

(ii) $e|a,\ e|b,$ $e|d.$

d $a,\ b$ 显 (i)

5, $s,\ t$

$$sa + tb = d.$$

$e|a,\ e|b$

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

(ii)

(i) (ii)

(i) d $a,\ b$

(ii) d $a,\ b$ $e|d$

$|e| \leq d.$

d $a,\ b$

* **8** $a,\ b$

(i) m $(am, bm) = (a, b)m.$

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

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

$d = (a, b),\ d' = (am, bm).$ 5, $s,\ t$

$sa + tb = d.$

端 $m,$ $s(am) + t(bm) = dm.$ $d'|dm.$

$dm|am,\ dm|bm.$ 7 (ii), $dm|d'.$

$d' = dm.$ (i)

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

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

$$(\frac{a}{d},\ \frac{b}{d}) = \frac{(a,b)}{|d|}. \qquad\qquad d = (a,\ b), \qquad (\frac{a}{(a,b)},\ \frac{b}{(a,b)}) = 1.$$

(ii)

21 $\quad a = 11 \cdot 200306,\ b = 23 \cdot 200306. \qquad (a,\ b).$

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

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

讨 n

$a_1,\ \ldots,\ a_n$ 递

化

9 $a_1,\ \ldots,\ a_n$ n $a_1 \neq 0.$

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

$(a_1, \ldots, a_n) = d_n$.

22 $(120, 150, 210, 35).$

$$(120, 150) = (120, 30) = 30,$$
$$(30, 210) = 30,$$
$$(30, 35) = (30, 5) = 5,$$

$$(120, 150, 210, 35) = 5.$$

***　　1**　　$a,\ b,\ c$　　$b \neq 0,\ c \neq 0.$　　$(a,c) = 1,$ $(ab,c) = (b,c).$

$d = (ab,c),\ d' = (b,c).$　　$d'|b,\ d'|c.$　　$d'|ab,\ d'|c.$　　§1.3 7,　　$d'|d.$

$(a,c) = 1,$　　§1.3　　6,　　$s,\ t$ $sa + tc = 1.$

$b,$　　$s(ab) + (tb)c \ = \ b.$　　§1.1　　3, $d|ab,\ d|c,$　　$d|s(ab) + (tb)c\ ,$　　$d|b.$　　§1.3　　7, $d|d'.$

$d = d'.$

$a,\ b,\ c$　　$c \neq 0.$　　$c|ab,\ (a,c) = 1\ ,$

$c|b$.

1, $c|(ab,c) = (b,c)$. $c|b$.

毕

1 $15|2\cdot 75$, $(2,15)=1$, $15|75$.

* **2** p $p|ab$, $p|a$ $p|b$.

$p \not| a$, §1.3 6, $(p,a)=1$. 1

$p|b$. 毕

2 $5|3\cdot 25$, $5 \not| 3$ 5 $5|25$.

问题: $c|ab$, $c|a$ $c|b$?

* **3** $a_1,\ \ldots,\ a_n,\ c$ $(a_i, c) = 1,\ 1 \leq i \leq n.$

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

* $a_1,\ \ldots,\ a_n$ p $p | a_1 \cdots a_n,$ p $a_k.$

* **1** $a_1, \ldots, a_n$ n m n

m n . $a_1, \ldots, a_n$

, $[a_1, \ldots, a_n]$.

$m = [a_1, \ldots, a_n]$

(i) $a_i | m,\ 1 \le i \le n$; (ii) $a_i | m',\ 1 \le i \le n,$ $m | m'$.

3 14 21 $\{\pm 42,\ \pm 84, \ldots\}$,

$[14, 21] = 42$.

* **4** $a,\ b$

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

4 $p,\ q$ $[p, q] = pq$.

* **5** $a,\ b$

(i) $a|m,\ b|m,$ $[a,b] \mid m;$ (ii) $[a,b] = \dfrac{ab}{(a,b)}.$

$d = (a,b).$ §1.3 8, $(\dfrac{a}{d}, \dfrac{b}{d}) = 1.$

4, $[\dfrac{a}{d}, \dfrac{b}{d}] = \dfrac{a}{d} \cdot \dfrac{b}{d},$ $[a,b] = \dfrac{ab}{d},$ (ii)

$\dfrac{a}{d} \mid \dfrac{m}{d},$ $\dfrac{b}{d} \mid \dfrac{m}{d},$ $\dfrac{a}{d} \cdot \dfrac{b}{d} \mid \dfrac{m}{d}.$ $\dfrac{ab}{d} \mid m,$ (i)

n $a_1,\ \ldots,\ a_n$

6 $a_1, \ldots, a_n$ n

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

$[a_1, \ldots, a_n] = m_n.$

5 $[120, 150, 210, 35].$

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

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

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

$$[120, 150, 210, 35] = 4200.$$

* **7** $a_1, \ a_2, \ \ldots, \ a_n$ $a_1|m, \ a_2|m, \ \ldots, \ a_n|m,$

$[a_1, a_2, \ldots, a_n] \mid m$

积 该

(积顺 情况).

* **1(术基本)** $n > 1$

积 积顺 情况 该

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

p_i $n = q_1 \cdots q_t,\ q_1 \leq \ldots \leq q_t, q_j$ $s = t,\ p_i = q_i,\ 1 \leq i \leq s.$

$n > 1$

积 (1) $n = 2, (1)$ $< n$

(1) $n,$

n (1) n n

$b,\ c$

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

$$b = p'_1 \cdots p'_u, \quad c = p'_{u+1} \cdots p'_s. \qquad n =$$

$p'_1 \cdots p'_s$. 适 变 p'_i (1) (1) n

(1) $n > 1$

还 $n = q_1 \cdots q_t$, $q_1 \leq \ldots \leq q_t$,

q_j

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

$p_1 | q_1 \cdots q_t$. §1.4 3 q_j $p_1 | q_j$.

p_1, q_j $p_1 = q_j$. p_k $q_1 = p_k$.

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

$p_1 = q_1$. (2) 消 p_1,

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

$p_2 = q_2$. 类 $p_3 = q_3, \ldots, q_s = p_t$. $s = t$.

1 $45,\ 49,\ 100,\ 128$

$1,$

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

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

幂 1

2 $n > 1$

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

$p_i < p_j\ (i < j)$

(3) n **标准分 式.**

2 $45,\ 49,\ 100,\ 128$ 标准

1 $1{,}45 = 3^2 \cdot 5, \quad 49 = 7^2, \quad 100 = 2^2 \cdot 5^2, \quad 128 = 2^7.$

便

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

3 n 1

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

d n d

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

4 $a,\ b$

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

a b

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

$a,\ b$ $(a, b)[a, b] = ab.$

4 $120,\ 150,\ 210,\ 35$

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

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

$120,\ 150,\ 210,\ 35$ $5.$

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

1.

2. 模　　价　　模

3. 模

4. 剩　　剩

5. 简　剩　　简　剩

6. 模　元

7.　　函

8.　　费马

9. RSA

10. 模重

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.

何判断 $a,\ b$ m 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 $a,\ b$ 表达形式来判断 $a,\ b$ m

理 1 设 m 设 $a,\ b$ $a \equiv b \pmod{m}$

充 条件 存 k 使得 $a = b + km.$

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

其次 具 种 **等价关系**

理 2 设 m m 等价关系 即

i). (自反) 任 $a,\ a \equiv a \pmod{m}$;

ii). (称) 若 $a \equiv b \pmod{m},$ $b \equiv a \pmod{m}$;

iii). (传递) 若 $a \equiv b \pmod{m},\ b \equiv c \pmod{m},$ $a \equiv c \pmod{m}.$

3 $39 \equiv 32 \pmod 7$, $32 \equiv 25 \pmod 7$, 所

$$39 \equiv 25 \pmod 7.$$

$$39 \equiv 39 \pmod 7, \qquad 25 \equiv 25 \pmod 7,$$

及

$$32 \equiv 39 \pmod 7, \qquad 25 \equiv 32 \pmod 7.$$

第三 运 $a,\ b$ m 可 $a,\ b$ m

3 m $a,\ b$ m 必

$a,\ b$ m 相

4 $39 \equiv 25 \pmod 7$, $39 = 5 \cdot 7 + 4$, $25 = 3 \cdot 7 + 4$.

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.

4 m $a_1,\ a_2,\ b_1,\ b_2$

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

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

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

$$\begin{aligned}
61 &= 39 + 22 \equiv 4 + 1 \equiv 5 \pmod{7},\\
17 &= 39 - 22 \equiv 4 - 1 \equiv 3 \pmod{7},\\
858 &= 39 \cdot 22 \equiv 4 \cdot 1 \equiv 4 \pmod{7},\\
1521 &= 39^2 \equiv 4^2 \equiv 2 \pmod{7},\\
484 &= 22^2 \equiv 1^2 \equiv 1 \pmod{7}.
\end{aligned}$$

6 2003 年 5 月 9 星期五 问 2^{2003} 天 星期几

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

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

故　2^{2003}　　二

下　　步

* **8**　$ad \equiv bd \pmod m$.　$(d, m) = 1$,　$a \equiv b \pmod m$.

证　$ad \equiv bd \pmod m$,　$m|ad - bd$,　$m|d(a - b)$. 从而 $m|a - b$.

11　$95 \equiv 25 \pmod 7$, $(5, 7) = 1$,　$19 \equiv 5 \pmod 7$.

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

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

13　$190 \equiv 50 \pmod{70}$,　取 $d = 10$,　到 $19 \equiv 5 \pmod 7$.

* **11**　$a \equiv b \pmod m$.　$d|m$,　$a \equiv b \pmod d$.

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

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

* **16**　p, q　不　素　　a, b 满足 $a \equiv b \pmod p, a \equiv b \pmod q$, $a \equiv b \pmod{pq}$.

$a \equiv b \pmod{p}$, $a \equiv b \pmod{p}$, $p|a-b$, $q|a-b$. $p,\ q$

$pq|a-b$. $a \equiv b \pmod{pq}$.

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

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.

意　　a, 令　$C_a = \{c \mid c \in \mathbf{Z},\ a \equiv c \pmod{m}\}$.

1 i)　　包含　　C_r　　$0 \le r \le m-1$.

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

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

1 C_a　　m　　a　　**剩　类**.　　剩

该　　**剩**　　**代表元**.　　$r_0, r_1, \ldots, r_{m-1}$　　m　　并且　　都　　剩　　里　　$r_0, \ldots, r_{m-1}$

m **完全** . m m

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

1 $a,\ C_a = \{a + 10k \mid k \in \mathbf{Z}\}$ $m = 10$

$0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9$ 10 完全

$1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10$ 10 完全

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

$0,\ 3,\ 6,\ 9,\ 12,\ 15,\ 18,\ 21,\ 24,\ 27$ 10 完全

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

2 m $r_0,\ r_1,\ \ldots,\ r_{m-1}$ m 完全

它 m

例 2 设 m 是一个正整数. 则

i) $0,\ 1,\ \ldots,\ m-1$ 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) $1,\ \ldots,\ m-1,\ m$ 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) $-(m-1),\ \ldots,\ -1,\ 0$ 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) $-m,\ -(m-1),\ \ldots,\ -1$ 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，$-m/2,\ -(m-2)/2,\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ (m-2)/2,$ 或 $-(m-2)/2,\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ (m-2)/2,\ m/2,$ 是模 m 的一个完全剩余系;

当 m 分别为奇数时，$-(m-1)/2,\ \ldots,\ -1,\ 0,\ 1,\ \ldots,\ (m-1)/2$

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**.

3 $(a,m)=1$, b x 遍历 m

$ax+b$ 也遍历 m

根据 2, 只需证明: $a_0,\ a_1,\ \ldots,\ a_{m-1}$ m

m $aa_0+b,\ aa_1+b,\ \ldots,\ aa_{m-1}+b$ m

事实上 a_i $a_j\ (i\neq j)$

$$aa_i+b\equiv aa_j+b\ (\mathrm{mod}\ m),$$

$m|a(a_i-a_j).$ $(a,m)=1$, 根据 §1.4 1 之推

$m|a_i-a_j$. 这说明 a_i 与 a_j m 与假 矛盾 此 $ax+b$ 也遍历 m

2 $m=10,\ a=7,\ b=5.$ $ax+b$ 10

5, 12, 19, 26, 33, 40, 47, 54, 61, 68 构成 10

4 $(m_1,\ m_2) = 1$. $x_1,\ x_2$ $m_1,\ m_2$

$m_2x_1 + m_1x_2$ m_1m_2

$x_1,\ x_2$ $m_1,\ m_2$ $m_2x_1 + m_1x_2$

m_1m_2 m_1m_2 m_1m_2

$x_1,\ x_2$ $y_1,\ y_2$

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

$m_2x_1+m_1x_2 \equiv m_2y_1+m_1y_2 \pmod{m_1}$, 者 $m_2x_1 \equiv m_2y_1 \pmod{m_1}$,

$m_1|m_2(x_1 - y_1)$. $(m_1, m_2) = 1$, $m_1|x_1 - y_1$. x_1

y_1 m_1

x_2 y_2 m_2 立 毕

3 $p,\ q$ $n = pq$. $c,$ 惟

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

$p,\ q$ $p,\ q$ 互

4 $x,\ y$ $p,\ q$ $qx + py$

$n = pq$ 惟 $x,\ y$

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

4 $m_1 = 2,\ m_2 = 5.$ $2x_1 + 5x_2$ 10

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

10

5 $m_1, m_2, \ldots, m_k$ k $x_1, x_2, \ldots, x_k$

$m_1, m_2, \ldots, m_k$

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

$$m_1 m_2 \cdots m_k$$

$a,\ m$ $(a,m)=1.$

m

1 m m $0,\ 1,\ \ldots,\ m-1$

m $\varphi(m),$ **欧拉** (Euler) **函数**.

1 $m=10.$ 10 $0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9$ 10

$1,\ 3,\ 7,\ 9,$ $\varphi(10)=4.$

2 m **简化** ,

m

1 $r_1,\ r_2$ m r_1 m

r_2 m

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

3 m 简化 每

组 集合 m .

m 简化 元 $\varphi(m)$.

3 $1,\ 3,\ 7,\ 9$ 10 简化 $\varphi(10) = 4.$

4 $1,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29$ 30 简化 $\varphi(30) = 8.$

5 $1,\ 2,\ 3,\ 4,\ 5,\ 6$ 7 简化 $\varphi(7) = 6.$

6 $m = p$ $1,\ 2,\ \ldots,\ p-1$ p 简化

$\varphi(p) = p - 1.$

2 $r_1,\ \ldots,\ r_{\varphi(m)}$ $\varphi(m)$ m

m $r_1,\ \ldots,\ r_{\varphi(m)}$ m 简化

依 $\varphi(m)$ $r_1,\ \ldots,\ r_{\varphi(m)}$ m

简化 $r_1,\ \ldots,\ r_{\varphi(m)}$ m 简化

3 $(a, m) = 1$. x m

ax m

$(a, m) = 1,\ (x, m) = 1,$ $(ax, m) = 1.$ ax

$ax_1 \equiv ax_2 \pmod{m}$ $x_1 \equiv x_2 \pmod{m}$.

x m ax $\varphi(m)$

m 2, ax m

7 $1,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29$ 30

$(7, 30) = 1$.

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

$7 \cdot 1,\ 7 \cdot 7,\ 7 \cdot 11,\ 7 \cdot 13,\ 7 \cdot 17,\ 7 \cdot 19,\ 7 \cdot 23,\ 7 \cdot 29$ 30

8 $m = 7$. a 示 列 m

x 示 m a x

列 交叉位置 示 ax m 最 负

列

$a \setminus x$	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

a 示 ax 随 x m

4 $(a,m)=1$. a', $1\le a'<m$

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

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 $x=a'$, $1\le a'<m$ 使得 aa' 属于 1 的剩余类, 即 $aa'\equiv 1 \pmod m$. 证毕.

际 体地求

广义欧 法 4 造

二 (造). $(a,m)=1$, §1.3 5, 广义欧 法 找 s, t $sa+tm=(a,m)=1$.

$a'=s \pmod m$ $aa'\equiv 1 \pmod m$.

9 $m=7$, a m 4,

$$1 \cdot 1 \equiv 1, \quad 2 \cdot 4 \equiv 1, \quad 3 \cdot 5 \equiv 1, \quad (\mathrm{mod}\ 7)$$
$$4 \cdot 2 \equiv 1, \quad 5 \cdot 3 \equiv 1, \quad 6 \cdot 6 \equiv 1, \quad (\mathrm{mod}\ 7).$$

10 $m = 737,\ a = 635.$ §1.3 19, 由

$$s = -224,\ t = 193$$

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

$$a' = -224 \equiv 513\ (\mathrm{mod}\ 737)$$

$$635 \cdot 513 \equiv 1\ (\mathrm{mod}\ 737).$$

5 $(m_1,\ m_2)=1$. $x_1,\ x_2$ m_1 m_2

$m_2x_1+m_1x_2$ m_1m_2

$(x_1,m_1)=1,\ (x_2,m_2)=1$ $(m_2x_1+m_1x_2,m_1m_2)=1.$

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 $(m_2x_1+m_1x_2,m_1m_2)=1.$

m_1m_2 $m_2x_1+m_1x_2,$

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.

5 拉函 φ (φ 谓 乘 函).

6 $m,\ n$ $\varphi(mn) = \varphi(m)\varphi(n)$.

5, x m 共 $\varphi(m)$

y n 共 $\varphi(m)$ $ym + xn$

mn $\varphi(m)\varphi(n)$. 但 mn

$\varphi(mn)$. $\varphi(mn) = \varphi(m)\varphi(n)$.

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

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

7 n 标准 解 $n = \Pi_{p|n} p^{\alpha} = p_1^{\alpha_1} \cdots p_k^{\alpha_s}$.

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

推论 $p,\ q$ $\varphi(pq) = pq - p - q + 1.$

明 7, $\varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1) = pq-p-q+1.$

n 道 n 很难

n 值 $\varphi(n)$.

13 n 积 道 n

值 $\varphi(n)$, n

考虑未 $p,\ q$ 方程

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

多项 间 方程

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

n p,q.

1 $m=7,\ a=2.$ $(2,7)=1,\ \varphi(7)=6.$

7 $1,\ 2,\ 3,\ 4,\ 5,\ 6,$

$$2\cdot 1\equiv 2,\ 2\cdot 2\equiv 4,\ 2\cdot 3\equiv 6,\ 2\cdot 4\equiv 1,\ 2\cdot 5\equiv 3,\ 2\cdot 6\equiv 5,\ (\mathrm{mod}\ 7).$$

述 左右

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

$$2^6\cdot 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\equiv 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\ (\mathrm{mod}\ 7).$$

注

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

$$2^6\equiv 1\ (\mathrm{mod}\ 7).$$

2 $m = 30,\ a = 7.$ $(7, 30) = 1,\ \varphi(30) = 8.$

30 $1,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,$

$7 \cdot 1 \equiv 7, \quad 7 \cdot 7 = 49 \equiv 19, \quad 7 \cdot 11 = 77 \equiv 17,$

$7 \cdot 13 = 91 \equiv 1, \quad 7 \cdot 17 = 119 \equiv 29, \ 7 \cdot 19 = 133 \equiv 13,$

$7 \cdot 23 = 161 \equiv 11, \ 7 \cdot 29 = 203 \equiv 23 \pmod{30}.$

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

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

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

1　　2　　般　结

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

$r_1,\ \ldots,\ r_{\varphi(m)}$　　m

a　　$(a,m)=1$　　$ar_1,\ \ldots,\ ar_{\varphi(m)}$　　m

就　　$ar_1,\ \ldots,\ ar_{\varphi(m)}$　　m

$r_1,\ \ldots,\ r_{\varphi(m)}$　　排　　$(ar_1)\cdots(ar_{\varphi(m)})$　　m

$r_1\cdots r_{\varphi(m)}$　　m

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

$r_1\cdots r_{\varphi(m)}\ (a^{\varphi(m)}-1)\ \equiv\ 0\ (\mathrm{mod}\ m).$　　$(r_1,m)\ =\ 1,\ \ldots,$ $(r_{\varphi(m)},m)=1$　　§1.4　　3,　　$(r_1\cdots r_{\varphi(m)},\ m)=1.$

§2.1　　8,　　$a^{\varphi(m)}-1\equiv 0 \pmod{m}$.

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

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

2 (Fermat) p a,

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

情

i) a p $a \equiv 0 \pmod{p}$ $a^p \equiv 0 \pmod{p}$.

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

ii) a p $(a, p) = 1$ (见 §1.3 4). 1,

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

端 a,

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

5 $p,\ q$ 奇 $n = pq$, a pq

e $1 < e < \varphi(n),\ (e, \varphi(n)) = 1,$ 那么

$d,\ 1 \le d < \varphi(n),$

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

$$a^e \equiv c \pmod{n}, \quad 1 \le c < n, \qquad c^d \equiv a \pmod{n}.$$

$(e, \varphi(n)) = 1,$ §2.3 4, $d,\ 1 \le d < \varphi(n),$

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

k $ed = 1 + k\ \varphi(n).$ 1 ,

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

$k(\varphi(n)/\varphi(p))$ 冪 a

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

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

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

p q §2.1 12 ,

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

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

3 (Wilson) p $(p-1)! \equiv -1 \pmod{p}$.

5 $p = 17$.

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

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

算术计算 大 m 大 n，计算 $b^n \pmod m$. 然 归 计算 $b^n \equiv (b^{n-1} \pmod m)\cdot b \pmod m$. 计算较 费 须 $n-1$ 将 n 写 制

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

$n_i \in \{0,1\},\ i = 0,1,\ldots,k-1.$ $b^n \pmod m$ 计算 归纳

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

$2[\log_2 n]$ 计算 “**模重复平方计算法**”. 算

0). $a = 1,$ 将 n 写 制 $n = n_0 + n_1 2 + \cdots + n_{k-1}2^{k-1},$

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

1). $n_0 = 1,$ $a_0 \equiv a \cdot b \pmod m,$ $a_0 = a.$

$a_0 \equiv a \cdot b^{n_0} \pmod m$. 再 $b_1 \equiv b^2 \pmod m$.

2). $n_1 = 1,$ $a_1 \equiv a_0 \cdot b_1 \pmod m,$ $a_1 = a_0.$

$a_1 \equiv a_0 \cdot b_1^{n_1} \pmod m$. 再 $b_2 \equiv b_1^2 \pmod m$. ……

k-1). $n_{k-2} = 1,$ $a_{k-2} \equiv a_{k-3} \cdot b_{k-2} \pmod m,$

$a_{k-2} = a_{k-3}.$ $a_{k-2} \equiv a_{k-3} \cdot b_{k-2}^{n_{k-2}} \pmod m$. 再

$b_{k-1} \equiv b_{k-2}^2 \pmod m$.

k). $n_{k-1} = 1,$ $a_{k-1} \equiv a_{k-2} \cdot b_{k-1} \pmod m,$

$a_{k-1} = a_{k-2}.$ $a_{k-1} \equiv a_{k-2} \cdot b_{k-1}^{n_{k-1}} \pmod m$.

后 a_{k-1} $b^n \pmod m$.

1 $12996^{227} \pmod{37909}$.

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

复平

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

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

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

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

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

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

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

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

$$12996^{227} \equiv 7775 \pmod{37909}.$$

本章主　讲　　题

1.　　基本

2.

3.　国

4.

5. $x^p - x$　　高

6. 高

7.　　提升

8.

m 况 ( ) .

1 m $f(x)$ $f(x) = a_n x^n + \cdots + a_1 x + a_0$,

a_i $f(x) \equiv 0 \pmod{m}$ (1)

m **式**. $a_n \not\equiv 0 \pmod{m}$, n $f(x)$ **次** ,

$\deg f$. (1) m n **次** **式**.

a $f(a) \equiv 0 \pmod{m}$ a (1)

. $x \equiv a \pmod{m}$ (1) a

$$C_a = \{c \mid c \in \mathbf{Z},\ a \equiv c \pmod{m}\}$$

(1) (1) a $x \equiv a \pmod{m}$.

在模 m 的完全剩余系中, 使得 (1) 成立的 (1) .

1 $x^5 + x + 1 \equiv 0 \pmod 7$ 1 7

$x \equiv 2 \pmod 7$

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

还 $x \equiv 2 \pmod 7$, 2.

1 $a \not| m$. $ax \equiv b \pmod{m}$ (2)

$(a,m)|b.$ (2) $d = (a,m).$

(2) $x \equiv x_0 \pmod{m}$, y_0

$ax_0 - my_0 = b.$ $(a,m)|a,\ (a,m)|m,$ $(a,m)|ax_0 - my_0 = b.$

$(a,m)|b.$ $\frac{b}{(a,m)}$

$$\frac{a}{(a,m)}x \equiv 1 \pmod{\frac{m}{(a,m)}}. \quad (3)$$

$(\frac{a}{(a,m)}, \frac{m}{(a,m)}) = 1,$ $x_0,$ (3)

(3) $x \equiv x_0 \pmod{\frac{m}{(a,m)}}.$ (4)

$\frac{a}{(a,m)}x \equiv 1 \pmod{\frac{m}{(a,m)}}$ $\frac{a}{(a,m)}x_0 \equiv 1 \pmod{\frac{m}{(a,m)}}$

减 $\frac{a}{(a,m)}(x-x_0)\equiv 0\ (\mathrm{mod}\ \frac{m}{(a,m)})$. $x\equiv x_0\ (\mathrm{mod}\ \frac{m}{(a,m)})$.

$$\frac{a}{(a,m)}x\equiv\frac{b}{(a,m)}\ (\mathrm{mod}\ \frac{m}{(a,m)}) \qquad (5)$$

$$x\equiv x_1\equiv x_0\frac{b}{(a,m)}\ (\mathrm{mod}\ \frac{m}{(a,m)}). \qquad (6)$$

$$x\equiv x_1\equiv x_0\frac{b}{(a,m)}\ (\mathrm{mod}\ m) \qquad (2)$$

(2) , $ax\equiv b\ (\mathrm{mod}\ m)$ 部

$$x\equiv x_1+t\frac{m}{(a,m)}\ (\mathrm{mod}\, m),\qquad t=0,\ 1,\ldots,\ (a,m)-1.$$

$ax\equiv b\ (\mathrm{mod}\ m)$ $ax_1\equiv b\ (\mathrm{mod}\ m)$,

减 $a(x-x_1)\equiv 0\ (\mathrm{mod}\ m)$. §2.1 10 8,

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

(2) 部 (7)

2 $33x \equiv 22 \pmod{77}$.

$(33, 77) = 11$, $(33, 77) = 11|22$, 原

$3x \equiv 1 \pmod{7}$

$x_0' \equiv 5 \pmod{7}$.

$3x \equiv 2 \pmod{7}$

$x_0 \equiv 2 \cdot x_0' \equiv 2 \cdot 5 \equiv 3 \pmod{7}$.

原

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

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

1, 更确切 描 §2.3 4.

2 $(a,m)=1$. $ax\equiv 1 \pmod m$ $x\equiv a' \pmod m$.

$(a,m)=1,\ b=1,$ $(a,m)|b.$

2 a a' $aa'\equiv 1 \pmod m$

a m **可逆** .

2, m a' a'

a m **逆** , $a'=a^{-1} \pmod m$.

m 逆 (2)

3 $(a,m)|b$. $ax\equiv b \pmod m$

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

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

4 m a m

a m

a m $(a, m) = 1$.

2, a' $aa' \equiv 1 \pmod{m}$.

2, a m

a m a'

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

$ax \equiv 1 \pmod{m}$ $x \equiv a' \pmod{m}$. 1,

$(a, m)|1$. $(a, m) = 1$. a m

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.

“物　　”

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

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.

$$2\cdot 5\cdot 7\cdot 2=140,\quad 1\cdot 3\cdot 7\cdot 3=63,\quad 1\cdot 3\cdot 5\cdot 2=30,$$
$$2\cdot 3\cdot 5\cdot 7=210,\quad 140+63+30=233,\quad 233-210=23.$$

$3,\ 5,\ 7$ 看 $m_1,\ m_2,\ m_3$; $2,\ 3,\ 2$ 看 $b_1,\ b_2,\ b_3$;
$5\cdot 7,\ 3\cdot 7,\ 3\cdot 5$ 看 $M_1,\ M_2,\ M_3$; $2,\ 1,\ 1$ 看 $M_1',\ M_2',\ M_3'$;
233 ; 105 $m=m_1\cdot m_2\cdot m_3$.

$$M_i'M_i\equiv 1\ (\mathrm{mod}\ m_i),\quad i=1,\ 2,\ 3,$$
$$x\equiv M_1'M_1b_1+\cdots+M_k'M_kb_k\ (\mathrm{mod}\ m).$$

1 (中国 **)** $m_1, \ldots, m_k$ k

$b_1, \ldots, b_k$,

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

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

(1)

$$x \equiv M_1' M_1 b_1 + \cdots + M_k' M_k b_k \pmod{m}, \qquad (2)$$

$$M_i' M_i \equiv 1 \pmod{m_i},\ i = 1, 2, \ldots, k.$$

(ii)

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

(1)

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

$N_i' N_i \equiv 1 \pmod{m_{i+1}},\ i = 1, 2, \ldots, k-1,$ x_i

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

$i = 1, \ldots, k,$

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

$i = 2, \ldots, k$

$x,\ x'$ (1)

$x \equiv b_i \equiv x' \pmod{m_i}, \quad i = 1, \ldots, k.$

$m_1,\ \ldots,\ m_k$ $x \equiv x' \pmod{m}$.

(i) 直接

$i,\ 1 \le i \le k,$ $(m_i, m_j) = 1,$

$1 \le j \le k,\ j \ne i,$ §1.4 3, $(m_i, M_i) = 1.$

$M_i',$ $M_i' M_i \equiv 1 \pmod{m_i},$

(2) $x = M_1' M_1 b_1 + \cdots + M_k' M_k b_k \pmod{m}.$

$m = m_i M_i$ $m_i | M_j,\ 1 \le j \le k,\ j \ne i,$ x

$x \equiv M_i' M_i b_i \equiv b_i \pmod{m_i}, \quad i = 1, \ldots, k.$

(2) (1)

1

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

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

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

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

$$M_i' M_i \equiv 1 \pmod{m_i}, \quad i = 1, 2, 3, 4.$$

$$M_1' = 3, \quad M_2' = 1, \quad M_3' = 1, \quad M_4' = 1.$$

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

2 韩信点兵　　兵　队　　纵队　　末　　人

六　纵队　　末　　人　　七　纵队　　末　四人

纵队　　末　　人　　兵

韩信点兵　　转

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

一　　$b_1 = 1,\ b_2 = 5,\ b_3 = 4,\ b_4 = 10$　　1,

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

:

$N_1 = 5.$ $x \equiv x_1 \equiv 1 \pmod 5,$

(y 待　参　) $x = 1 + 5y.$　　x 代入

$1 + 5y \equiv 5 \pmod 6,$　　$5y \equiv 4 \pmod 6.$

$N_1 = 5$　　$m_2 = 6,$　　$N_1' \equiv N_1^{-1} \equiv 5 \pmod 6,$

$y \equiv 5{\cdot}4 \equiv 2 \pmod 6.$　　$x = x_2 = 1{+}5{\cdot}2 \equiv 11 \pmod{30}.$

(y 待　参　)$x = x_2 = 11 + 30y.$ 代入

$11 + 30y \equiv 4 \pmod 7,$　　$30y \equiv 4 - 11 \equiv 0 \pmod 7.$

$N_2 = 30$　　$m_3 = 7,$　　$N_2' \equiv N_2^{-1} \equiv 4 \pmod 7,$

$y \equiv 4{\cdot}0 \pmod 7.$　　$x = x_3 = 11{+}30{\cdot}0 \equiv 11 \pmod{210}.$

(y 待　参　) $x = x_3 = 11 + 210y.$ 代入

$$11 + 210y \equiv 10 \pmod{11}, \qquad 210y \equiv 10 - 11 \equiv 10 \pmod{11}.$$

$$N_3 = 210 \qquad m_4 = 11,$$

$$N_3' \equiv N_3^{-1} \equiv 1 \pmod{11},$$

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

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

3 $2^{1000000} \pmod{77}$.

利 Euler

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 $a_0 = a \equiv 1, \quad b_1 \equiv b^2 \equiv 4 \pmod{77}$.

2). $n_1 = 0$. 计算 $a_1 = a_0 \equiv 1, \quad b_2 \equiv b_1^2 \equiv 16 \pmod{77}$.

3). $n_2 = 0$. 计算 $a_2 = a_1 \equiv 1, \quad b_3 \equiv b_2^2 \equiv 25 \pmod{77}$.

4). $n_3 = 1$. 计算 $a_3 = a_2 \cdot b_3 \equiv 25, \quad b_4 \equiv b_3^2 \equiv 9 \pmod{77}$.

5). $n_4 = 0$. 计算 $a_4 = a_3 \equiv 25, \quad b_5 \equiv b_4^2 \equiv 4 \pmod{77}$.

6). $n_5 = 1$. 计算 $a_5 = a_4 \cdot b_5 \equiv 23 \pmod{77}$.

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

$x = 2^{1000000}$. $77 = 7 \cdot 11$, $x \pmod{77}$

$$\begin{cases} x \equiv b_1 \pmod 7 \\ x \equiv b_2 \pmod{11}. \end{cases}$$

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

似 $2^{\varphi(11)} \equiv 2^{10} \equiv 1 \pmod{11}$, $1000000 = 100000 \cdot 10$,

$b_2 \equiv 2^{1000000} \equiv (2^{10})^{100000} \equiv 1 \pmod{11}$.

$m_1 = 7,\ m_2 = 11,\ m = m_1 \cdot m_2 = 77,\ M_1 = m_2 = 11,\quad M_2 = m_1 = 7,\quad 11M_1' \equiv 1 \pmod 7,\quad 7M_2' \equiv 1 \pmod{11}$.

$M_1' = 2,\quad M_2' = 8$.

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

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

2 1 $b_1, \ldots, b_k$ $m_1, \ldots, m_k$

$$x \equiv M_1' M_1 b_1 + \cdots + M_k' M_k b_k \pmod{m}$$

$m = m_1 \cdots m_k$

$x_0 = M_1' M_1 b_1 + \cdots + M_k' M_k b_k \pmod{m}$, $b_1, \ldots, b_k$ $m_1, \ldots, m_k$ x_0 $m_1 \cdots m_k$

能够 m

$$M_1' M_1 b_1 + \cdots + M_k' M_k b_k \equiv M_1' M_1 b_1' + \cdots + M_k' M_k b_k' \pmod{m},$$

§2.1 11, $M_i' M_i b_i \equiv M_i' M_i b_i' \pmod{m_i}, \quad i = 1, \ldots, k.$

$M_i' M_i \equiv 1 \pmod{m_i}, \quad i = 1, \ldots, k$, $b_i \equiv b_i' \pmod{m_i}, \ i = 1, \ldots, k.$ $b_i, \ b_i'$

$$b_i = b_i', \quad i = 1, \ldots, k.$$

1　　$m_1,\ \ldots,\ m_k$　　$m = m_1 \cdots m_k$.

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

T_i　　$f(x) \equiv 0 \pmod{m_i}$　　T　　(1)　　$T = T_1 \cdots T_k$.

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

1

$$\begin{cases} f(x) \equiv 0 \pmod 5, \\ f(x) \equiv 0 \pmod 7. \end{cases}$$

验

$f(x) \equiv 0 \pmod 5$ $x \equiv 1,\ 4 \pmod 5$,

$f(x) \equiv 0 \pmod 7$ $x \equiv 3,\ 5,\ 6 \pmod 7$.

$$\begin{cases} x \equiv b_1 \pmod 5 \\ x \equiv b_2 \pmod 7 \end{cases}$$

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

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

$2 \cdot 3 = 6$

$m = \Pi_p p^\alpha$, $f(x) \equiv 0 \pmod{m}$,

$f(x) \equiv 0 \pmod{p^\alpha}$.

p $f(x) \equiv 0 \pmod{p^\alpha}$ (3)

$f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$

$f'(x) = n a_n x^{n-1} + \cdots + 2a_2 x + a_1$. $f'(x)$ $f(x)$ **导** .

2 $x \equiv x_1 \pmod{p}$ $f(x) \equiv 0 \pmod{p}$ (4)

$(f'(x_1), p) = 1$, (3) $x \equiv x_\alpha \pmod{p^\alpha}$,

x_α

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

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

2 $f(x) \equiv x^4 + 7x + 4 \equiv 0 \pmod{27}$.

(按照 2)

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

$f(x) \equiv 0 \pmod{3}$ $x_1 \equiv 1 \pmod{3}$.

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

$f(1) \equiv 3 \pmod{9}$, $f'(1) \equiv 2 \pmod{9}$,

$3 + 3t_1 \cdot 2 \equiv 0 \pmod{9}$ $2t_1 \equiv -1 \pmod{3}$. $t_1 \equiv 1 \pmod{3}$,

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

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

$f(4) \equiv 18 \pmod{27}$, $f'(4) \equiv 20 \pmod{27}$,

$18 + 9t_2 \cdot 20 \equiv 0 \pmod{27}$ $2t_2 \equiv -2 \pmod{3}$. $t_2 \equiv 2 \pmod{3}$,

$f(x) \equiv 0 \pmod{27}$ $x_3 \equiv 4 + 9t_2 \equiv 22 \pmod{27}$.

(2)

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

$$f(x) \equiv 0 \pmod 3 \qquad x_1 \equiv 1 \pmod 3.$$

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

$$\begin{cases} t_1 \equiv -\dfrac{f(x_1)}{3^1}(f'(x_1)^{-1} \pmod 3) \equiv 1 \pmod 3, \\ \\ x_2 \equiv x_1 + 3t_1 \equiv 4 \pmod 9; \end{cases}$$

$$\begin{cases} t_2 \equiv -\dfrac{f(x_2)}{3^2}(f'(x_1)^{-1} \pmod 3) \equiv 2 \pmod 3, \\ \\ x_3 \equiv x_2 + 3^2 t_2 \equiv 22 \pmod{27}. \end{cases}$$

$$f(x) \equiv 0 \pmod{27} \qquad x_3 \equiv 22 \pmod{27}.$$

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

引　(　　)　$f(x) = a_n x^n + \cdots + a_1 x + a_0$

n　　$g(x) = x^m + \cdots + b_1 x + b_0$　　$m \geq 1$

$q(x)$　　$r(x)$

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

(I) $n < m$.　　$q(x) = 0,\ r(x) = f(x),$

(II) $n \geq m$.　　$f(x)$　　n　　$n = m$.

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

$q(x) = a_n x,\ r(x) = f(x) - a_n x \cdot g(x)$

$n - 1 \geq m$

$n > m$,

$$f(x) - a_n x^{n-m} \cdot g(x)$$

$$= (a_{n-1} - a_n b_{m-1})x^{n-1} + \cdots + (a_{n-m} - a_n b_0)x^{n-m}$$

$$+ a_{n-m-1}x^{n-m-1} + \cdots + a_0.$$

$f(x) - a_n x^{n-m} \cdot g(x)$ $\leq n - 1$

(I), $q_1(x)$ $r_1(x)$

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

$q(x) = a_n x^{n-m} + g_1(x),\ r(x) = r_1(x)$

$x^p - x \pmod p$ 零 借助

超 $p - 1$

1 (1) $p-1$ p

$q(x),\ r(x)$ $f(x) = (x^p - x)q(x) + r(x)$,

$\deg r(x) \leq p-1$. x, $x^p - x \equiv 0 \pmod{p}$.

$f(x) \equiv 0 \pmod{p}$ $r(x) \equiv 0 \pmod{p}$.

1 $3x^{14} + 4x^{13} + 2x^{11} + x^9 + x^6 + x^3 + 12x^2 + x \equiv 0 \pmod{5}$ < 5

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

$$3x^3 + 16x^2 + 6x \equiv 0 \pmod{5}.$$

2 $1 \le k \le n.$ $x \equiv a_i \pmod{p}$ (1) k

$x,$ $f(x) \equiv (x-a_1)\cdots(x-a_k)f_k(x) \pmod{p},$ (2)

$f_k(x)$ $n-k$ $a_n.$

2

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

p 界估

4 (1)

$< p$ p

p

5 $n \le p$. $f(x) = x^n + \cdots + a_1 x + a_0 \equiv 0 \pmod{p}$, (3)

n $x^p - x$ $f(x)$

p 倍

p d $p-1$ $x^d - 1$

p d

$d|p-1$, q $p - 1 = dq$.

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

5, $x^d - 1$ p d

3 $2x^3+5x^2+6x+1 \equiv 0 \pmod 7$

5, 变 $4 \cdot 2 \equiv 1 \pmod 7$, $4(2x^3+5x^2+6x+1) \equiv x^3-x^2+3x-3 \pmod 7$.

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

5, 3.

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

去掉 7 $2x^{15}-x^{10}+4x-3 \equiv \pmod 7$.

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

$$x^4 - 2x^3 - 4x + 3 \equiv 0 \pmod 7.$$

$x = 0, \pm1, \pm2, \pm3,$ 无

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

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

$$3x^3+16x^2+6x \equiv 3x^3+x^2+x \pmod 5.$$

$$x \equiv 0,\ 1,\ 2 \pmod 5.$$

恒 $x^p - x \equiv 0 \pmod p$,

$t, k,\ x^{t+k(p-1)} \equiv x^t \pmod p$. $(p=5)$,

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

$$3x^3+16x^2+6x \equiv 0 \pmod 5.$$

$$2(3x^3+16x^2+6x) \equiv x^3+2x^2+2x \equiv 0 \pmod 5.$$

$$x \equiv 0,\ 1,\ 2 \pmod 5.$$

1.

2.

3. 勒让　符号　　律

4.

5.　斯引　　律

6. 雅克比符号

7.　p

8. 椭圆曲线

二次同余式的一般形式是　$ax^2+bx+c\equiv 0\ (\mathrm{mod}\ m)$　(1)　$m\not| a.$

$$m=p_1^{\alpha_1}\cdots p_k^{\alpha_k},\qquad (1)$$

$$\begin{cases} ax^2+bx+c\equiv 0\ (\mathrm{mod}\ p_1^{\alpha_1}),\\ \qquad\qquad\cdots\cdots\\ ax^2+bx+c\equiv 0\ (\mathrm{mod}\ p_k^{\alpha_k}). \end{cases}$$

p^α　$ax^2+bx+c\equiv 0\ (\mathrm{mod}\ p^\alpha),\quad p\not| a.\quad (2)$

(2)　$4a,$　$4a^2x^2+4abx+4ac\equiv 0\ (\mathrm{mod}\ p^\alpha)$

$(2ax+b)^2\equiv b^2-4ac\ (\mathrm{mod}\ p^\alpha).$　$y=2ax+b,$

$$y^2\equiv b^2-4ac\ (\mathrm{mod}\ p^\alpha).$$

p　$(p,2a)=1.$　(2).

1 $x^2 \equiv a \pmod{m}, \quad (a,m) = 1 \quad (3)$

a m ( );

a m **非** (**非**).

问题: 1) a m $\sqrt{a}$ 什 区

2) (3) 3) (3)

1 1 4 -1 4

2 $1,\ 2,\ 4$ 7 $-1,\ 3,\ 5$ 7

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

3 $-1,\ 1,\ 2,\ 4,\ 8,\ 9,\ 13,\ 15$ 17

$3,\ 5,\ 6,\ 7,\ 10,\ 11,\ 12,\ 14$ 17

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

4 $E : y^2 = x^3 + x + 1 \pmod 7$

$x = 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6, \qquad y.$

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

$x = 1,\ y^2 = 3 \pmod 7, \qquad ,$

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

$x = 3,\ y^2 = 3 \pmod 7, \qquad ,$

$x = 4,\ y^2 = 6 \pmod 7, \qquad ,$

$x = 5,\ y^2 = 5 \pmod 7, \qquad ,$

$x = 6,\ y^2 = 6 \pmod 7, \qquad .$

5 $E : y^2 = x^3 + x + 2 \pmod 7$

$x = 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6\ ,$ $y.$

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

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

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

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

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

$x = 5,\ y^2 = 6 \pmod 7, \quad ,$

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

p　　$x^2 \equiv a \pmod{p}, \quad (a,p)=1. \quad (1)$

1 (　　)　p　　$(a,p)=1.$

(i) a　　p　　$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}; \quad (2)$

(ii) a　　p　　$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}. \quad (3)$

a　　p　　(1)

(i)　　p

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

$q(x)$　　x

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) p $(a,p)=1$,

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

§1.4 2, $p|a^{\frac{p-1}{2}}-1$ $p|a^{\frac{p-1}{2}}+1$. (i)
告诉 a p $a^{\frac{p-1}{2}}\equiv -1\,(\mathrm{mod}\,p)$.

p $(a_1,p)=1,\ (a_2,p)=1$.

(i) $a_1,\ a_2$ p a_1a_2 p

(ii) $a_1,\ a_2$ p a_1a_2 p

(iii) a_1 p a_2 p a_1a_2 p

$$(a_1a_2)^{\frac{p-1}{2}}=a_1^{\frac{p-1}{2}}\cdot a_2^{\frac{p-1}{2}},$$

1

1 137 227

1, $137^{(227-1)/2} = 137^{113} \pmod{227}$.

$m = 227,\ b = 137.$ $a = 1.$ 113

$113 = 1 + 2^4 + 2^5 + 2^6.$

1). $n_0 = 1.$ $a_0 = a \cdot b^{n_0} \equiv 137, \quad b_1 \equiv b^2 \equiv 155 \pmod{227}.$

2). $n_1 = 0.$ $a_1 = a_0 \cdot b_1^{n_1} \equiv 137, \quad b_2 \equiv b_1^2 \equiv 190 \pmod{227}.$

3). $n_2 = 0.$ $a_2 = a_1 \cdot b_2^{n_2} \equiv 137, \quad b_3 \equiv b_2^2 \equiv 7 \pmod{227}.$

4). $n_3 = 0.$ $a_3 = a_2 \cdot b_3^{n_3} \equiv 137, \quad b_4 \equiv b_3^2 \equiv 49 \pmod{227}.$

5). $n_4 = 1.$ $a_4 = a_3 \cdot b_4^{n_4} \equiv 130, \quad b_5 \equiv b_4^2 \equiv 131 \pmod{227}.$

6). $n_5 = 1.$ $a_5 = a_4 \cdot b_5^{n_5} \equiv 5, \quad b_6 \equiv b_5^2 \equiv 136 \pmod{227}.$

7). $n_6 = 1.$ $a_6 = a_5 \cdot b_6^{n_6} \equiv 226 \equiv -1 \pmod{227}.$

137 227

2 p p

各 $(p-1)/2$, $(p-1)/2$ 序

$1^2,\ 2^2,\ \ldots,\ (\frac{p-1}{2})^2$ (4) 仅

§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.

1　　p　　勒让得 (Legendre) 符号

$$\left(\frac{a}{p}\right)=\begin{cases}1, & a \quad p\\ -1, & a \quad p\\ 0, & p|a.\end{cases}$$

1　　§4.1　　3,

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

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

§4.2 1 叙

1 (判别 则) a, $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$.

2 2 17 3 17

$(17-1)/2 = 2^3$, $2^2 \equiv 4,\ 2^4 \equiv 4^2 \equiv -1,\ 2^8 \equiv (-1)^2 \equiv 1;$

$3^2 \equiv 9,\ 3^4 \equiv 9^2 \equiv -4,\ 3^8 \equiv (-4)^2 \equiv -1 \pmod{17}$.

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

2 p $\left(\frac{-1}{p}\right) = \begin{cases} 1, & p \equiv 1 \pmod{4}; \\ -1, & p \equiv 3 \pmod{4}. \end{cases}$

2 p (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) $(a,p) = 1$, $\left(\frac{a^2}{p}\right) = 1$.

(i) $x^2 \equiv a+p \pmod{p}$

$x^2 \equiv a \pmod{p}$, $\left(\frac{a+p}{p}\right) = \left(\frac{a}{p}\right)$.

(ii) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$, $\left(\frac{b}{p}\right) \equiv^{\frac{p-1}{2}} \pmod{p}$

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

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

± 1, p $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

p $a \equiv b \pmod{p}$, $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

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.

(Gauss) p $(a,p)=1.$ $a\cdot 1,\ a\cdot 2,\ \ldots,\ a\cdot\dfrac{p-1}{2}$

p $\dfrac{p}{2}$ $m,$ $\left(\dfrac{a}{p}\right)=(-1)^m.$

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

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

p

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

3 (i),

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

$p \equiv \pm 1 \pmod 8$, k $p = 8k \pm 1$.

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

$p \equiv \pm 3 \pmod 8$, k $p = 8k \pm 3$.

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

4 ( ) $p,\ q$

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

3 2 17 3 17

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

2 17

4,

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

2 (i) 1 1 (ii), $\left(\frac{17}{3}\right) = \left(\frac{-1}{3}\right) = (-1)^{\frac{3-1}{2}} = -1,$

$\left(\frac{3}{17}\right) = -1$, 3 17

4 $x^2 \equiv 137 \pmod{227}$

227 2 ,

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

3 (i),

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

4 3 (i),

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

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

5 $x^2 \equiv -1 \pmod{365}$

$365 = 5 \cdot 73$

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

$\left(\frac{-1}{5}\right) = \left(\frac{-1}{73}\right) = 1,$ 4.

6 $x^2 \equiv 2 \pmod{3599}$

$3599 = 59 \cdot 61$

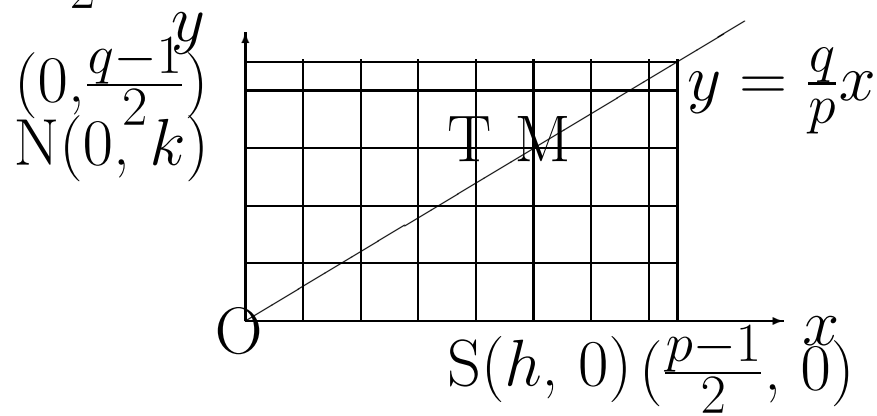
$$\begin{cases} x^2 \equiv 2 \pmod{59}, \\ x^2 \equiv 2 \pmod{61}. \end{cases}$$

$\left(\frac{2}{59}\right) = (-1)^{(59^2-1)/8} = -1,$

§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 $\left(\frac{q}{p}\right)=(-1)^{\Sigma_{h=1}^{\frac{p-1}{2}}\left[\frac{qh}{p}\right]}$,　　$\left(\frac{p}{q}\right)=(-1)^{\Sigma_{k=1}^{\frac{q-1}{2}}\left[\frac{pk}{q}\right]}$,

所以只需证明 $\Sigma_{h=1}^{\frac{p-1}{2}}\left[\frac{qh}{p}\right]+\Sigma_{k=1}^{\frac{q-1}{2}}\left[\frac{pk}{q}\right]=\frac{p-1}{2}\cdot\frac{q-1}{2}$.



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 $[\frac{qh}{p}]$, 因此，下三角形内的整点个数为 $\sum_{h=1}^{\frac{p-1}{2}}\left[\frac{qh}{p}\right]$;

水平 NM $[\frac{pk}{q}]$,

$\sum_{k=1}^{\frac{q-1}{2}} \left[\frac{pk}{q}\right]$.

对 无

$$\sum_{h=1}^{\frac{p-1}{2}} \left[\frac{qh}{p}\right] + \sum_{k=1}^{\frac{q-1}{2}} \left[\frac{pk}{q}\right] = \frac{p-1}{2}\frac{q-1}{2}.$$

这就完成了定理 . 毕.

例 1 求　　奇素　p, 它　3　其二次剩余

解 即　求　　奇素　p, 使得 $\left(\frac{3}{p}\right)=1$.

根据二次互反律　$\left(\frac{3}{p}\right)=(-1)^{(p-1)/2}\left(\frac{p}{3}\right)$.

$$(-1)^{(p-1)/2}=\begin{cases}1, & \text{当 } p\equiv 1 \pmod 4;\\ -1, & \text{当 } p\equiv -1 \pmod 4,\end{cases}$$ 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 $\left(\frac{-1}{p}\right)=1$　充　条件是 $\begin{cases}p\equiv 1 \pmod 4\\ p\equiv 1 \pmod 6\end{cases}$ 或 $\begin{cases}p\equiv -1 \pmod 4\\ p\equiv -1 \pmod 6.\end{cases}$

分别等价于 $p\equiv 1 \pmod{12}$, 或 $p\equiv -1 \pmod{12}$.

3 是模 p 二次剩余　充分必　条件是 $p\equiv \pm 1 \pmod{12}$.

2 设 p d 如果 $\left(\frac{d}{p}\right)=-1$, 则 p 一 不能表示 x^2-dy^2 式

如果 p 表达式 $p=x^2-dy^2$, 则由 p 可 到 $(x,p)=(y,p)=1$. 事实 若 $(x,p)\neq 1$, 则

$$p|x, \quad p|x^2-p=dy^2.$$

但 $(d,p)=1$, $p|y^2$, 进而 $p|y$. 样 $p^2|x^2$, $p^2|y^2$. 从而 $p^2|x^2-dy^2=p$. 不可能

$$\left(\frac{d}{p}\right)=\left(\frac{d}{p}\right)\left(\frac{y^2}{p}\right)=\left(\frac{dy^2}{p}\right)=\left(\frac{x^2}{p}\right)=1.$$

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.

义 1 $m = p_1 \cdots p_r$ p_i 乘积 任意 a,

义 **雅可比 (Jacobi) 符号**

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right) \cdots \left(\frac{a}{p_r}\right).$$

雅 比符号 勒让 符号 推广 蕴含 意义已经 同 雅 比符号 -1, 判断 a m 非 ; 雅比符号 1, 却 判断 a m 例 3 119 非

$$\left(\frac{3}{119}\right) = \left(\frac{3}{7}\right)\left(\frac{3}{17}\right) = (-1)(-1) = 1.$$

1 m 正

(i) $\left(\dfrac{a+m}{m}\right)=\left(\dfrac{a}{m}\right)$;

(ii) $\left(\dfrac{ab}{m}\right)=\left(\dfrac{a}{m}\right)\left(\dfrac{b}{m}\right)$; (iii) $(a,m)=1$, $\left(\dfrac{a^2}{m}\right)=1$.

$m=p_1\cdots p_r$, 中 p_i

(i) $\left(\frac{a+m}{m}\right)=\left(\frac{a+m}{p_1}\right)\cdots\left(\frac{a+m}{p_r}\right)=\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)=\left(\dfrac{a}{m}\right)$.

$$(ii)\quad \left(\frac{ab}{m}\right)=\left(\frac{ab}{p_1}\right)\cdots\left(\frac{ab}{p_r}\right)=\left(\frac{a}{p_1}\right)\left(\frac{b}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_r}\right)$$

$$=\left(\frac{a}{p_1}\right)\cdots\left(\frac{a}{p_r}\right)\left(\frac{b}{p_1}\right)\cdots\left(\frac{b}{p_r}\right)=\left(\frac{a}{m}\right)\left(\frac{b}{m}\right).$$

(iii) $\left(\frac{a^2}{m}\right)=\left(\frac{a^2}{p_1}\right)\cdots\left(\frac{a^2}{p_r}\right)=1.$

引　：　$m = p_1 \cdots p_r$

$$\frac{m-1}{2} \equiv \frac{p_1 - 1}{2} + \cdots + \frac{p_r - 1}{2} \pmod 2;$$

$$\frac{m^2-1}{8} \equiv \frac{p_1^2 - 1}{8} + \cdots + \frac{p_r^2 - 1}{8} \pmod 2.$$

2　m　(i) $\left(\dfrac{1}{m}\right) = 1;$

(ii) $\left(\dfrac{-1}{m}\right) = (-1)^{\frac{m-1}{2}};$　(iii) $\left(\dfrac{2}{m}\right) \equiv (-1)^{\frac{m^2-1}{8}}$

3　m, n 都　$\left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}} \left(\frac{m}{n}\right).$

1

$$x^2 \equiv 286 \pmod{563}$$

否　解

用　虑 563　否　　接计算

$$\left(\frac{286}{563}\right) = \left(\frac{2}{563}\right)\left(\frac{143}{563}\right) = (-1)^{\frac{563^2-1}{8}}(-1)^{\frac{143-1}{2}\cdot\frac{563-1}{2}}\left(\frac{563}{143}\right) = \left(\frac{-9}{143}\right) = \left(\frac{-1}{143}\right) = -1,$$

原　　解

2 出 $y^2 \equiv x^3 + x + 1 \pmod{17}$ 及
令 $f(x) = x^3 + x + 1$. §4.1 3, 我们

$f(0) = 1$, $y = 1,\ y = 16$; $f(1) = 3$, 无解;
$f(2) = 11$, 无解 $f(3) = 14$, 无解;
$f(4) = 1$, $y = 1,\ y = 16$; $f(5) = 12$, 无解;
$f(6) = 2$, $y = 6,\ y = 11$; $f(7) = 11$, 无解;
$f(8) = 11$, 无解; $f(9) = 8$, $y = 5,\ y = 12$;
$f(10) = 8$, $y = 5,\ y = 12$; $f(11) = 0,\ y = 0$;
$f(12) = 7$, 无解; $f(13) = 1,\ y = 1,\ y = 16$;
$f(14) = 5$, 无解; $f(15) = 8,\ y = 5,\ y = 12$;
$f(16) = -1,\ y = 4,\ y = 13 \pmod{17}$.

$$(0,1),\ (0,16),\ (4,1),\ (4,16),\ (6,6),\ (6,11),\ (9,5),\ (9,12),$$
$$(10,5),\ (10,12),\ (11,0),\ (13,1),\ (13,16),\ (15,5),\ (15,12),\ (16,4),\ (16,13).$$

p 给 a, 应 高斯 (§4.3 4) 快速地 a p

$$x^2 \equiv a \pmod{p}$$

也 说 存 性

现 情况 a 满足

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

情况 具体 过程按照 面法 行

p , 将 $p-1$ 写 $p-1=2^t\cdot s,\ t\geq 1,$ s

(i) 选取 p $n,$ n $\left(\frac{n}{p}\right)=-1.$

再 $b:=n^s \pmod p.$ $b^{2^t}\equiv 1,$ $b^{2^{t-1}}\equiv -1 \pmod p.$

b p 2^t 单位 p 2^{t-1} 单位

(ii) $x_{t-1}:=a^{\frac{s+1}{2}} \pmod p.$ $a^{-1}x_{t-1}^2$

$y^{2^{t-1}}\equiv 1 \pmod p,$ $a^{-1}x_{t-1}^2$ p 2^{t-1} 单位

$$(a^{-1}x_{t-1}^2)^{2^{t-1}}\equiv a^{2^{t-1}s}\equiv a^{(p-1)/2}\equiv\left(\frac{a}{p}\right)\equiv 1 \pmod p.$$

(iii) $t=1,$ $x=x_{t-1}=x_0\equiv a^{\frac{s+1}{2}} \pmod p$ $x^2\equiv a \pmod p.$

$t\geq 2,$ 寻找 x_{t-2} $a^{-1}x_{t-2}^2$ $y^{2^{t-2}}\equiv 1 \pmod p.$

$a^{-1}x_{t-2}^2$ p 2^{t-2} 单位

x_{t-2} $a^{-1}x_{t-2}^2$ $y^{2^{t-2}} \equiv 1 \pmod{p}$.

(a) $(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv 1 \pmod{p}$,

$j_0 := 0,\ x_{t-2} := x_{t-1} = x_{t-1}b^{j_0} \pmod{p}$, x_{t-2}

(b) $(a^{-1}x_{t-1}^2)^{2^{t-2}} \equiv -1 \equiv (b^{-2})^{2^{t-2}} \pmod{p}$,

$j_0 := 1,\ x_{t-2} := x_{t-1}b = x_{t-1}b^{j_0} \pmod{p}$, x_{t-2}

去 ....

假 x_{t-k} $a^{-1}x_{t-k}^2$ $y^{2^{t-k}} \equiv 1 \pmod{p}$,

$a^{-1}x_{t-k}^2$ p 2^{t-k} $(a^{-1}x_{t-k}^2)^{2^{t-k}} \equiv 1 \pmod{p}$.

(k+2) $t = k$, $x = x_{t-k} \pmod{p}$ $x^2 \equiv a \pmod{p}$.

$t \geq k+1$, x_{t-k-1} $a^{-1}x_{t-k-1}^2$

$y^{2^{t-k-1}} \equiv 1 \pmod{p}$. $a^{-1}x_{t-k-1}^2$ p 2^{t-k-1}

x_{t-k-1} $a^{-1}x_{t-k-1}^2$ $y^{2^{t-k-1}} \equiv 1 \pmod{p}$.

(a) $(a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv 1 \pmod{p}$,

$j_{k-1} := 0, \quad x_{t-k-1} := x_{t-k} = x_{t-k} b^{j_{k-1}2^{k-1}} \pmod{p}$,

x_{t-k-1}

(b) $(a^{-1}x_{t-k}^2)^{2^{t-k-1}} \equiv -1 \equiv (b^{-2^k})^{2^{t-k-1}} \pmod{p}$,

$j_{k-1} := 1, \; x_{t-k-1} := x_{t-k} b^{2^{k-1}} = x_{t-k} b^{j_{k-1}2^{k-1}} \pmod{p}$,

x_{t-k-1} 特 $k = t-1$,

$$x = x_0 \equiv x_1 b^{j_{t-2}2^{t-2}} \equiv \ldots \equiv x_{t-1} b^{j_0 + j_1 2 + \cdots + j_{t-2}2^{t-2}}$$

$$\equiv a^{\frac{s+1}{2}} b^{j_0 + j_1 2 + \cdots + j_{t-2}2^{t-2}} \pmod{p}$$

$x^2 \equiv a \pmod{p}$.

1 述 $x^2 \equiv 186 \pmod{401}$.

$$a = 186 = 2 \cdot 3 \cdot 31,$$

$$\left(\frac{2}{401}\right) = (-1)^{(401^2-1)/8} = 1, \qquad \left(\frac{3}{401}\right) = (-1)^{\frac{3-1}{2}\frac{401-1}{2}} \left(\frac{401}{3}\right) = \left(\frac{-1}{3}\right) = -1,$$

$$\left(\frac{31}{401}\right) = (-1)^{\frac{31-1}{2}\frac{401-1}{2}} \left(\frac{401}{31}\right) = \left(\frac{-2}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{2}{31}\right) = (-1)^{\frac{31-1}{2}}(-1)^{\frac{31^2-1}{8}} = -1,$$

$$\left(\tfrac{186}{401}\right) = \left(\tfrac{2}{401}\right)\left(\tfrac{3}{401}\right)\left(\tfrac{31}{401}\right) = 1 \cdot (-1) \cdot (-1) = 1.$$

$p = 401\ , \qquad p - 1 = 400 = 2^4 \cdot 25, \qquad t = 4,\ s = 25$

(i) $401 \qquad n = 3, \qquad n = 3 \qquad \left(\frac{3}{403}\right) = -1.$

$b := 3^{25} \equiv 268 \pmod{401}.$

(ii) $x_3 := 186^{\frac{25+1}{2}} \equiv 103 \pmod{401}. \qquad a^{-1} \equiv 235 \pmod{401}.$

(iii) $(a^{-1}x_3^2)^{2^2} \equiv 98^4 \equiv -1 \pmod{401},$

$j_0 := 1,\ x_2 := x_3 b^{j_0} = 103 \cdot 268 \equiv 336 \pmod{401},$

(iv) $(a^{-1}x_2^2)^2 \equiv (-1)^2 \equiv 1 \pmod{401},$

$j_1 := 0,\ x_1 := x_2 b^{j_1 2} = 336 \pmod{401}.$

(v) $a^{-1}x_1^2 \equiv -1 \pmod{401},$

$j_2 := 1,\ x_0 := x_1 b^{j_2 2^2} = 336 \cdot 268^4 \equiv 304 \pmod{401},$

$x \equiv x_0 \equiv 304 \pmod{p}$

$$x^2 \equiv 186 \pmod{401}.$$

2 p $4k+3$ $x^2 \equiv a \pmod{p}$

$x \equiv \pm a^{(p+1)/4} \pmod{p}$.

p $4k+3$ q $p-1=2q$.

$x^2 \equiv a \pmod{p}$

$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$,

者 $a^q \equiv 1 \pmod{p}$.

两端 时 a,

$$a^{q+1} \equiv a \pmod{p}.$$

$$x \equiv \pm a^{\frac{q+1}{2}} \equiv \pm a^{(p+1)/4} \pmod{p}.$$

3 $p,\ q$ $4k+3$ a $\left(\frac{a}{p}\right)=\left(\frac{a}{q}\right)=1,$ $x^2\equiv a\ (\mathrm{mod}\ pq).$

$x^2\equiv a\ (\mathrm{mod}\ pq)$ 组 $\begin{cases} x^2\equiv a\ \ (\mathrm{mod}\ p) \\ x^2\equiv a\ \ (\mathrm{mod}\ q), \end{cases}$

$x^2\equiv a\ (\mathrm{mod}\ p)$ $x\equiv \pm a^{(p+1)/4}\ (\mathrm{mod}\ p),$

$x^2\equiv a\ (\mathrm{mod}\ q)$ $x\equiv \pm a^{(q+1)/4}\ (\mathrm{mod}\ q),$

§3.2 1(国),

$$x\equiv \pm(a^{\frac{p+1}{4}}\ (\mathrm{mod}\ p))uq \pm (a^{\frac{q+1}{4}}\ (\mathrm{mod}\ q))vp\ (\mathrm{mod}\ pq),$$

$u,\ v$

$$uq\equiv 1\ (\mathrm{mod}\ p),\quad vp\equiv 1\ (\mathrm{mod}\ q).$$

本章　讨论　主　　容

1.

2. 指

3. 基本　质 (循环群)

4.

5.　　构造　生　元　构造

6. 指标

7. n

8.　　构造

步 $x^n \equiv a \pmod{m}$. (1)

$m > 1$ $(a, m) = 1$. 欧拉 $a^{\varphi(m)} \equiv 1 \pmod{m}$.

问该 $\varphi(m)$ 立 最小 最小

哪些

1 $m > 1$ a m

$$a^e \equiv 1 \pmod{m}$$

立 最小 e 叫做 a m **指数**. 记作 $\mathrm{ord}_m(a)$.

a m $\varphi(m)$, a 叫做 m **原根**.

1 $m = 7.\ \varphi(7) = 6.$ $1^1 \equiv 1,\ 2^3 = 8 \equiv 1,\ 3^3 = 27 \equiv -1,$
$4^3 \equiv (-3)^3 \equiv 1, 5^3 \equiv (-2)^3 \equiv -1,\ 6^2 \equiv (-1)^2 \equiv 1 \pmod 7.$

列

a	1	2	3	4	5	6
$\mathrm{ord}_m(a)$	1	3	6	3	6	2

$3,\ 5$ 7 $2,\ 4,\ 6$ 7

2 $m = 14 = 2 \cdot 7,$ $\varphi(14) = 6.$

$1^1 \equiv 1,$ $3^3 = 27 \equiv -1,$ $5^3 = 125 \equiv -1,$
$9^3 \equiv (-5)^3 \equiv 1,\ 11^3 \equiv (-3)^3 \equiv 1,\ 13^2 \equiv (-1)^2 \equiv 1 \pmod{14}.$

列

a	1	3	5	9	11	13
$\mathrm{ord}_m(a)$	1	6	6	3	3	2

$3,\ 5$ 14 $9,\ 11,\ 13$ 14

3 $m = 15 = 3 \cdot 5, \qquad \varphi(15) = 8.$

$1^1 \equiv 1, \qquad 2^4 = 16 \equiv 1, \qquad 4^2 = 16 \equiv 1, \qquad 7^2 = 49 \equiv 4, \qquad 7^4 \equiv 16 \equiv 1,$

$8^4 \equiv (-7)^4 \equiv 1, \ 11^2 \equiv (-4)^2 \equiv 1, \ 13^4 \equiv (-2)^4 \equiv 1, \ 14^2 \equiv (-1)^2 \equiv 1 \pmod{15}.$

a	1	2	4	7	8	11	13	14
$\mathrm{ord}_m(a)$	1	4	2	4	4	2	4	2

没 15

4 $m = 9 = 3^2, \qquad \varphi(9) = 6.$

$1^1 \equiv 1, \qquad 2^3 = 8 \equiv -1, \qquad 4^3 = 64 \equiv 1,$

$5^3 \equiv (-4)^3 \equiv -1, \ 7^3 \equiv (-2)^3 \equiv 1, \ 8^2 \equiv (-1)^2 \equiv 1 \pmod{9}.$

a	1	2	4	5	7	8
$\mathrm{ord}_m(a)$	1	6	3	6	3	2

2, 5 9

5 $m = 8 = 2^3$, $\varphi(8) = 4$.

$$1^1 \equiv 1,\ 3^2 = 9 \equiv 1,\ 5^2 = 25 \equiv 1,\ 7^2 \equiv (-1)^2 \equiv 1 \pmod 8.$$

a	1	3	5	7
$\mathrm{ord}_m(a)$	1	2	2	2

8

6 5 3 6 $3^2,\ 2\cdot 3^2$

$\varphi(3) = 2$, 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 $\varphi(3^2) = 6$, 且

$$5 \equiv 5,\ 5^2 \equiv 7,\ 5^3 \equiv 8 \equiv -1, 5^4 \equiv 4,\ 5^5 \equiv 2,\ 5^6 \equiv 1 \pmod{3^2};$$

$2 \cdot 3^2$, $(5, 2) = 1$,

$$5 \equiv 5,\ 5^2 \equiv 7,\ 5^3 \equiv 8 \equiv -1, 5^4 \equiv 4,\ 5^5 \equiv 2,\ 5^6 \equiv 1 \pmod{2 \cdot 3^2}.$$

1 $(a,m)=1$. d $a^d \equiv 1 \pmod{m}$

$\mathrm{ord}_m(a)|d.$

$\mathrm{ord}_m(a)|d,$ k $d = k\ \mathrm{ord}_m(a).$

$a^d = (a^{\mathrm{ord}_m(a)})^k \equiv 1 \pmod{m}.$

$\mathrm{ord}_m(a)|d$ 几里 除

$q,\ r$ $d = \mathrm{ord}_m(a)q + r, \quad 0 < r < \mathrm{ord}_m(a).$

$a^r \equiv a^r(a^{\mathrm{ord}_m(a)})^q = a^d \equiv 1 \pmod{m}.$

$\mathrm{ord}_m(a)$ $\mathrm{ord}_m(a)|d.$

推论 1 $m > 1$ a m $\mathrm{ord}_m(a)|\varphi(m).$

1, a m $\mathrm{ord}_m(a)$ $\varphi(m)$

$\varphi(m)$ $\mathrm{ord}_m(a).$

7 5 17 $\mathrm{ord}_{17}(5)$.

$\varphi(17) = 16$, 16 $d = 1,\ 2,\ 4,\ 8,\ 16$,

$a^d \pmod m$.

$5^1 \equiv 5,\ 5^2 = 25 \equiv 8,\ 5^4 \equiv 64 \equiv 13 \equiv -4, 5^8 \equiv (-4)^2 \equiv 16 \equiv -1,\ 5^{16} \equiv (-1)^2 \equiv 1 \pmod{17}$,

$\mathrm{ord}_{17}(5) = 16$. 5 17

2 p $(p-1)/2$ $(a,p) = 1$

, a 1 p $\mathrm{ord}_p(a) = \frac{p-1}{2}$ $p-1$.

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

$1,\ \mathrm{ord}_p(a)$ $\varphi(p) = p - 1 = 2 \cdot \dfrac{p-1}{2}$

$\mathrm{ord}_m(a) \neq 2$, $\mathrm{ord}_p(a) = \frac{p-1}{2}$ $p-1$.

性质 1　　$(a, m) = 1$.

(i)　　$b \equiv a \pmod{m}$,　　$\mathrm{ord}_m(b) = \mathrm{ord}_m(a)$.

(ii)　　a^{-1}　　$a^{-1}a \equiv 1 \pmod{m}$,　　$\mathrm{ord}_m(a^{-1}) = \mathrm{ord}_m(a)$.

8 39　　17　　$\mathrm{ord}_{17}(39) = \mathrm{ord}_{17}(5) = 16$.

7　　17　　16.　　$5^{-1} \equiv 7 \pmod{m}$.

2　　$(a, m) = 1$.　　$1 = a^0,\ a,\ \ldots,\ a^{\mathrm{ord}_m(a)-1}$　　m

当 a　　m　　$\mathrm{ord}_m(a) = \varphi(m)$

$\varphi(m)$　　m　简化　　系

$\mathrm{ord}_m(a)$　　$a^0,\ a,\ \ldots,\ a^{\mathrm{ord}_m(a)-1}$

m　　$0 \le k,\ l < \mathrm{ord}_m(a)$

$$a^k \equiv a^l \pmod{m}.$$

妨　　$k > l$.　　$a^{-1} \pmod{m}$,　　$a^{k-l} \equiv 1 \pmod{m}$.

$0 < k - l < \mathrm{ord}_m(a)$. $\mathrm{ord}_m(a)$ 结

a m $\mathrm{ord}_m(a) \;=\; \varphi(m)\;,$ $\varphi(m)$

$1 = a^0,\ a,\ \ldots,\ a^{\varphi(m)-1}$ m

§2.3 2, $\varphi(m)$ m

9 $\{5^k \mid k = 0, \ldots, 15\}$ 17

$5^0 \equiv 1$, $5^1 \equiv 5$, $5^2 = 25 \equiv 8$,

$5^3 \equiv 8 \cdot 5 \equiv 6$, $5^4 \equiv 8^2 \equiv 13$, $5^5 \equiv 13 \cdot 5 \equiv 14$,

$5^6 \equiv 6^2 \equiv 2$, $5^7 \equiv 2 \cdot 5 \equiv 10$, $5^8 \equiv 10 \cdot 5 \equiv 40 \equiv -1$

$5^9 \equiv (-1) \cdot 5 \equiv 12$, $5^{10} \equiv (-1) \cdot 8 \equiv 9$, $5^{11} \equiv (-1) \cdot 6 \equiv 11$,

$5^{12} \equiv (-1) \cdot 13 \equiv 4$, $5^{13} \equiv (-1) \cdot 14 \equiv 3$, $5^{14} \equiv (-1) \cdot 2 \equiv 15$,

$5^{15} \equiv (-1) \cdot 10 \equiv 7 \pmod{17}$.

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

3 $(a,m)=1$. $a^d \equiv a^k \pmod{m} \Leftrightarrow d \equiv k \pmod{\mathrm{ord}_m(a)}$.

10 $2^{1000000} \equiv 2^{10} \equiv 100 \pmod{231}$. $\mathrm{ord}_{231}(2) = 30$, $1000000 \equiv 10 \pmod{30}$.

11 $2^{2002} \equiv 2^1 \equiv 2 \pmod{7}$. $\mathrm{ord}_7(2) = 3$, $2002 \equiv 1 \pmod{3}$.

4 $(a,m)=1$. $d \geq 0$ $\mathrm{ord}_m(a^d) = \frac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a),d)}$.

12 $5^2 \equiv 8 \pmod{17}$ 17 $\mathrm{ord}_{17}(5^2) = \dfrac{\mathrm{ord}_{17}(5)}{(\mathrm{ord}_{17}(5),2)} = 8$.

$m > 1$ g m $d \geq 0$

g^d 仅 $(d, \varphi(m)) = 1.$

4,

$$\mathrm{ord}_m(g^d) = \frac{\mathrm{ord}_m(g)}{(\mathrm{ord}_m(g), d)} = \frac{\varphi(m)}{(\varphi(m), d)}.$$

g^d $\mathrm{ord}_m(g^d) = \varphi(m)$ 仅 $(d, \varphi(m)) = 1.$

5 m g, m $\varphi(\varphi(m))$

g m $\varphi(m)$

$$g,\ g^2,\ \ldots,\ g^{\varphi(m)}$$

m

又 g^d m $(d, \varphi(m)) = 1$.

d 共 $\varphi(\varphi(m))$ m $\varphi(\varphi(m))$

13 17

7 知道 5 17 5, $\varphi(\varphi(17)) = \varphi(16) = 8$ 5, $5^3 \equiv 6,\ 5^5 \equiv 14,\ 5^7 \equiv 10,\ 5^9 \equiv 12,\ 5^{11} \equiv 11,\ 5^{13} \equiv 3,\ 5^{15} \equiv 7 \pmod{17}$ 17 全部

6 $(ab,m)=1,\ (a,\ b)=1$. $(\mathrm{ord}_m(a),\mathrm{ord}_m(b))=1,$ $\mathrm{ord}_m(ab)=\mathrm{ord}_m(a)\mathrm{ord}_m(b)$. 之亦然

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

$$a^{\mathrm{ord}_m(b)\mathrm{ord}_m(ab)} \equiv (a^{\mathrm{ord}_m(b)})^{\mathrm{ord}_m(ab)}(b^{\mathrm{ord}_m(b)})^{\mathrm{ord}_m(ab)}$$
$$\equiv ((ab)^{\mathrm{ord}_m(ab)})^{\mathrm{ord}_m(b)} \equiv 1 \pmod m,$$

$\mathrm{ord}_m(a) \mid \mathrm{ord}_m(b)\mathrm{ord}_m(ab).$ $(\mathrm{ord}_m(a),\mathrm{ord}_m(b))=1,$ §1.4 1 之 $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(ab).$

$\mathrm{ord}_m(b) \mid \mathrm{ord}_m(ab).$ $(\mathrm{ord}_m(a),\mathrm{ord}_m(b))=1$ §1.4 4, $\mathrm{ord}_m(a)\mathrm{ord}_m(b) \mid \mathrm{ord}_m(ab).$

另 $(ab)^{\mathrm{ord}_m(a)\mathrm{ord}_m(b)} = (a^{\mathrm{ord}_m(a)})^{\mathrm{ord}_m(b)}(b^{\mathrm{ord}_m(b)})^{\mathrm{ord}_m(a)} \equiv 1 \pmod m,$ $\mathrm{ord}_m(ab) \mid \mathrm{ord}_m(a)\mathrm{ord}_m(b).$

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

来 $\mathrm{ord}_m(ab) = \mathrm{ord}_m(a)\mathrm{ord}_m(b)$, 那么

$$(ab)^{[\mathrm{ord}_m(a),\mathrm{ord}_m(b)]} = a^{[\mathrm{ord}_m(a),\mathrm{ord}_m(b)]}\ b^{[\mathrm{ord}_m(a),\mathrm{ord}_m(b)]} \equiv 1 \pmod{m},$$

$$\mathrm{ord}_m(ab)|[\mathrm{ord}_m(a), \mathrm{ord}_m(b)],$$

$$\mathrm{ord}_m(a)\mathrm{ord}_m(b)|[\mathrm{ord}_m(a), \mathrm{ord}_m(b)].$$

$$(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1.$$

14 71

2 71 $\mathrm{ord}_{71}(2) = 35;$

-2 71

-2 71 $\mathrm{ord}_{71}(-2) = \mathrm{ord}_{71}(-1)\mathrm{ord}_{71}(2) = 70.$

7 $m,\ n$ 大 1 $(a, m) = 1$.

(i) $n|m$, $\mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$.

(ii) $(m, n) = 1$, $\mathrm{ord}_{mn}(a) = [\mathrm{ord}_m(a), \mathrm{ord}_n(a)]$.

(i) $\mathrm{ord}_m(a)$ $a^{\mathrm{ord}_m(a)} \equiv 1 \pmod{m}$.

$n|m$ $a^{\mathrm{ord}_m(a)} \equiv 1 \pmod{n}$. $\mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$.

(ii) (i) $\mathrm{ord}_m(a) \mid \mathrm{ord}_{mn}(a)$, $\mathrm{ord}_n(a) \mid \mathrm{ord}_{mn}(a)$,

$[\mathrm{ord}_m(a), \mathrm{ord}_n(a)] \mid \mathrm{ord}_{mn}(a)$.

$a^{[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]} \equiv 1 \pmod{m}$, $a^{[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]} \equiv 1 \pmod{n}$,

$a^{[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]} \equiv 1 \pmod{mn}$.

$\mathrm{ord}_{mn}(a) \mid [\mathrm{ord}_m(a), \mathrm{ord}_n(a)]$. $\mathrm{ord}_{mn}(a) = [\mathrm{ord}_m(a), \mathrm{ord}_n(a)]$.

1 $p,\ q$ a pq

$\mathrm{ord}_{pq}(a) = [\mathrm{ord}_p(a), \mathrm{ord}_q(a)]$.

15 $p \neq q$ $n = pq$, $(a, p) = 1$. e

$1 < e < \varphi(n)$, $(e, \varphi(n)) = 1$, $d = d_a$, $1 \leq d < \mathrm{ord}_n(a)$,

$ed \equiv 1 \pmod{\mathrm{ord}_n(a)}$.

$$a^e \equiv c \pmod{n}, \quad 1 \leq c < n, \qquad c^d \equiv a \pmod{n}.$$

$$(e, \varphi(n)) = 1,\ \mathrm{ord}_n(a) \mid \varphi(n), \qquad (e, \mathrm{ord}_{pq}(a)) = 1.$$

$d = d_a$, $1 \leq d < \mathrm{ord}_n(a)$, $ed \equiv 1 \pmod{\mathrm{ord}_n(a)}$.

k $ed = 1 + k\ \mathrm{ord}_{pq}(a)$.

$$a^{\mathrm{ord}_p(a)} \equiv 1 \pmod{p}.$$

$(\mathrm{ord}_{pq}(a)/\mathrm{ord}_p(a))$ $k(\mathrm{ord}_{pq}(a)/\mathrm{ord}_p(a))$ 幂

并 a $a^{1+k\ \mathrm{ord}_{pq}(a)} \equiv a \pmod{p}$, $a^{ed} \equiv a \pmod{p}$.

$a^{ed} \equiv a \pmod{q}$. p 和 q §2.1

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

2 $(a,m)=1$. $m=2^n p_1^{\alpha_1}\cdots 2p_k^{\alpha_k}$

$$\mathrm{ord}_m(a)=[\mathrm{ord}_{2^n}(a),\mathrm{ord}_{p_1^{\alpha_1}}(a),\ldots,\mathrm{ord}_{p_k^{\alpha_k}}(a)].$$

8 $(m,n)=1$. mn $a_1,\ a_2,$

a $\mathrm{ord}_{mn}(a)=[\mathrm{ord}_m(a_1),\mathrm{ord}_n(a_2)]$.

$$\begin{cases} x\equiv a_1 \pmod m,\\ x\equiv a_2 \pmod n. \end{cases}$$

惟 $x\equiv a \pmod{mn}$.

1 (i), $\mathrm{ord}_m(a)=\mathrm{ord}_m(a_1),\quad \mathrm{ord}_n(a)=\mathrm{ord}_n(a_2)$.

7 , $\mathrm{ord}_{mn}(a)=[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]=[\mathrm{ord}_m(a_1),\mathrm{ord}_n(a_2)]$.

注 $m,$ $\mathrm{ord}_m(ab)=[\mathrm{ord}_m(a),\mathrm{ord}_m(b)]$

2, $\mathrm{ord}_{10}(3\cdot 3)=2\neq[\mathrm{ord}_{10}(3),\mathrm{ord}_{10}(3)]=4$, $\mathrm{ord}_{10}(3\cdot 7)=1\neq[\mathrm{ord}_{10}(3),\mathrm{ord}_{10}(7)]=4$. $\mathrm{ord}_{10}(7\cdot 9)=4=[\mathrm{ord}_{10}(7),\mathrm{ord}_{10}(9)]=4$.

9 m $a,\ b,$ c

$$\mathrm{ord}_m(c) = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)].$$

§1.5 5, $\mathrm{ord}_m(a)$ $\mathrm{ord}_m(b),$ $u,\ v$

$u|\mathrm{ord}_m(a), \quad v|\mathrm{ord}_m(b), \quad (u,v) = 1$

$[\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)] = uv.$

$s = \frac{\mathrm{ord}_m(a)}{u}, \quad t = \frac{\mathrm{ord}_m(b)}{v},$

4,

$$\mathrm{ord}_m(a^s) = \frac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), s)} = u, \quad \mathrm{ord}_m(b^t) = v.$$

6,

$$\mathrm{ord}_m(a^s b^t) = \mathrm{ord}_m(a^s)\mathrm{ord}_m(b^t) = uv = [\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)].$$

$c = a^s b^t \pmod m$.

16 $m = 3631$. m

$\varphi(3631) = 3630 = 2 \cdot 3 \cdot 5 \cdot 11^2$,

$\mathrm{ord}_{3631}(2) = 605 = 5 \cdot 11^2$, $\mathrm{ord}_{3631}(3) = 1210 = 2 \cdot 5 \cdot 11^2$,

$\mathrm{ord}_{3631}(5) = 363 = 3 \cdot 11^2$, $\mathrm{ord}_{3631}(6) = 1210 = 2 \cdot 5 \cdot 11^2$,

$\mathrm{ord}_{3631}(7) = 33 = 3 \cdot 11$, $\mathrm{ord}_{3631}(10) = 1815 = 3 \cdot 5 \cdot 11^2$,

$\mathrm{ord}_{3631}(11) = 330 = 2 \cdot 3 \cdot 5 \cdot 11$, $\mathrm{ord}_{3631}(12) = 1210 = 2 \cdot 5 \cdot 11^2$,

$\mathrm{ord}_{3631}(13) = 1815 = 3 \cdot 5 \cdot 11^2$, $\mathrm{ord}_{3631}(14) = 1815 = 3 \cdot 5 \cdot 11^2$,

$\mathrm{ord}_{3631}(15) = 3630 = 2 \cdot 3 \cdot 5 \cdot 11^2$, $\mathrm{ord}_{3631}(17) = 1210 = 2 \cdot 5 \cdot 11^2$.

9, $a = 3,\ b = 5$ $u = 1210,\ v = 33$,

$s = 1,\ t = 11^2$, $c = a^s b^t = 3^1 \cdot 5^{121} \equiv 2623 \pmod{3631}$

$$[\mathrm{ord}_{3631}(3), \mathrm{ord}_{3631}(3)] = [1210, 363] = 3630.$$

$c = 2623$ 3631

先　　m　　p

1　p　　p

—(　　)　　p　　$1,\ \ldots,\ p-1$

$e_r = \mathrm{ord}_p(r), \quad 1 \le r \le p-1, \qquad e = [e_1, \ldots, e_{p-1}].$

§5.1　　8,　　g,　　$g^e \equiv 1 \pmod{p}$.

$e|\varphi(p) = p-1.$　　$e_r|e, \quad r = 1, \ldots, p-1,$

$x^e \equiv 1 \pmod{p}$　　$p-1$　　$x \equiv 1,\ \ldots,\ p-1 \pmod{p}$.

§3.4　　4,　　$p-1 \le e.$　　g　　$p-1,$　　g

p

二( ) $d|p-1$. $F(d)$ p

d $F(d)=\varphi(d)$.

$\Sigma_{d|p-1}F(d)=p-1$ $\Sigma_{d|p-1}\varphi(d)=p-1$

$\Sigma_{d|p-1}(\varphi(d)-F(d))=0$.

$F(d)\le\varphi(d)$, $d|p-1$, $F(d)=\varphi(d)$.

$F(p-1)=\varphi(p-1)$. p $p-1$

p $F(d)=\varphi(d)$.

因为模 p 指数为 d 的元素满足： $x^d-1\equiv 0\ (\mathrm{mod}\ p)$, (2)

且当 a 是模 p 指数为 d 的元素， (2) 的解可以表示成 $x\equiv a^0,\ a,\ \ldots,\ a^{d-1}$.

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 $F(d)\le\varphi(d)$.

p $d|p-1$. p d

2 g p g $g+p$ p^2

g p^2 n. $g^n \equiv 1 \pmod{p^2}$, $n \mid \varphi(p^2) = p(p-1)$.

$g^n \equiv 1 \pmod{p}$ g $p-1 = \mathrm{ord}_p(g) \mid n$.

$n = p-1$ $n = p(p-1)$. $n = p(p-1) = \varphi(p^2)$,

g p^2 $n = p-1$, $g^{p-1} \equiv 1 \pmod{p^2}$.

$g+p$ p^2

$$(g+p)^{p-1} = g^{p-1} + (p-1)g^{p-2}p + \binom{p}{2} g^{p-3}p^2 + \ldots + p^{p-1}$$
$$\equiv g^{p-1} + (p-1)g^{p-2}p \pmod{p^2}.$$

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，$\mathrm{ord}_{p^2}(g+p) = p(p-1) = \varphi(p^2)$. $g+p$ 是模 p^2 的原根.

3 p α, p^α 更确切 g p^2 α, g p^α p^2 g $g^{p-1} \not\equiv 1 \pmod{p^2}$.

α 学归纳 $g^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha}$. $(*)$

$\alpha = 2$ 时, 命题成立. 假设 $\alpha \geq 2$ 时, 命题成立, 即 $g^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha}$.

关 $g^{p^{\alpha-2}(p-1)} = 1 + u_{\alpha-2}p^{\alpha-1}, \quad p \not| u_{\alpha-2}.$

p

$$\begin{aligned} g^{p^{\alpha-1}(p-1)} &= 1 + \binom{p}{1} u_{\alpha-2}p^{\alpha-1} + \binom{p}{2} (u_{\alpha-2}p^{\alpha-1})^2 + \cdots + (u_{\alpha-2}p^{\alpha-1})^p \\ &\equiv 1 + u_{\alpha-2}p^\alpha \pmod{p^{\alpha+1}}. \qquad (**) \end{aligned}$$

$p \not| u_{\alpha-2}$, $g^{p^{\alpha-1}(p-1)} \not\equiv 1 \pmod{p^{\alpha+1}}$. $(*)$ $\alpha + 1$

学归纳 关 $(*)$ $\alpha \geq 2$

g p^α d, $g^d \equiv 1 \pmod{p^\alpha}$, $g^d \equiv 1 \pmod{p^2}$.

g p^2 g p^2 $p(p-1) = \varphi(p^2) | d$.

$d | \varphi(p^\alpha)$. d $d = p^{r-1}(p-1), \quad 2 \le r \le \alpha$.

代入 (**),

$$1 + u_{r-1}p^r = g^{p^{r-1}(p-1)} \equiv 1 \pmod{p^\alpha}$$

$$u_{r-1}p^r \equiv 0 \pmod{p^\alpha}.$$

$p \not| u_{r-1}$, $r \ge \alpha$. $r = \alpha$. g p^α

4 $\alpha \geq 1$, g p^α g $g + p^\alpha$ $2p^\alpha$

(i) a $a^d \equiv 0 \pmod{p^\alpha}$,

显 $a^d \equiv 0 \pmod{2}$,

§2.1 12, $a^d \equiv 0 \pmod{2p^\alpha}$. 显

(ii) g $d = \varphi(p^\alpha)$, $\varphi(2p^\alpha) = \varphi(p^\alpha) = d$.

$g^d \equiv 1 \pmod{p^\alpha}$, $g^r \not\equiv 1 \pmod{p^\alpha}$, $0 < r < d$

$g^d \equiv 1 \pmod{2p^\alpha}$, $g^r \not\equiv 1 \pmod{2p^\alpha}$, $0 < r < d$.

g $2p^\alpha$

(iii) g 偶 $g + p^\alpha$ (ii)

5 a $\alpha \geq 3$,

$$a^{\varphi(2^\alpha)/2} \equiv a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}.$$

a $a = 2b + 1$,

$a^2 = 4b(b+1) + 1 \equiv 1 \pmod{2^3}$. $\alpha = 3$

$\alpha - 1$, $a^{2^{(\alpha-1)-2}} \equiv 1 \pmod{2^{\alpha-1}}$

$t_{\alpha-3}$ $a^{2^{(\alpha-1)-2}} = 1 + t_{\alpha-3}2^{\alpha-1}$.

$$a^{2^{\alpha-2}} = (1 + 2^{\alpha-1}t_{\alpha-3})^2 = 1 + (t_{\alpha-3} + 2^{\alpha-2}t_{\alpha-3}^2)2^\alpha \equiv 1 \pmod{2^\alpha}.$$

α (10)

$\alpha \geq 3$

6 $\alpha \geq 3$. $\mathrm{ord}_{2^\alpha}(5) = \varphi(2^\alpha)/2 = 2^{\alpha-2}$.

5, $5^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}$. $\mathrm{ord}_{2^\alpha}(5) \mid 2^{\alpha-2}$.

$\mathrm{ord}_{2^\alpha}(5) \nmid 2^{\alpha-3}$.

$5^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \pmod{2^\alpha}$.

α

$\alpha = 3$ $5^{2^{3-3}} \equiv 1 + 2^2 \pmod{2^3}$.

$\alpha \geq 3$ 命 $5^{2^{\alpha-3}} \equiv 1 + 2^{\alpha-1} \pmod{2^\alpha}$.

q $5^{2^{\alpha-3}} = 1 + 2^{\alpha-1} + q2^\alpha$.

$$5^{2^{(\alpha+1)-3}} = (1+2^{\alpha-1})^2 + 2(1+2^{\alpha-1})q2^\alpha + (q2^\alpha)^2 = 1 + 2^\alpha + (2^{\alpha-3} + q + q2^{\alpha-1} + q^2 2^{\alpha-1})2^{\alpha+1}.$$

$5^{2^{(\alpha+1)-3}} \equiv 1 + 2^{(\alpha+1)-1} \pmod{2^{\alpha+1}}$. $\alpha+1$

根据归纳法原理, 关系式对所有 $\alpha \geq 3$ 成立. $\mathrm{ord}_{2^\alpha}(5) = 2^{\alpha-2} = \varphi(2^\alpha)/2$.

7 m $\Leftrightarrow m=2,\ 4,\ p^\alpha,\ 2p^\alpha,$ p

m 准 $m=2^\alpha p_1^{\alpha_1}\cdots 2p_k^{\alpha_k}.$

$(a,m)=1,$ $(a,2^\alpha)=1,\quad (a,p_i^{\alpha_i})=1,\quad i=1,\ldots,k.$

根据欧拉定理及定理 5,
$$\begin{cases} a^{\tau} & \equiv 1 \pmod{2^\alpha} \\ a^{\varphi(p_1^{\alpha_1})} & \equiv 1 \pmod{p_1^{\alpha_1}} \\ & \vdots \\ a^{\varphi(p_k^{\alpha_k})} & \equiv 1 \pmod{p_k^{\alpha_k}}, \end{cases} \qquad \tau=\begin{cases} \varphi(2^\alpha), & \alpha\le 2, \\ \frac{1}{2}\varphi(2^\alpha), & \alpha\ge 3. \end{cases}$$

$h=[\tau,\ \varphi(p_1^{\alpha_1}),\ \ldots,\ \varphi(p_k^{\alpha_k})].$ §5.1 6

$a,\ (a,m)=1,$ $a^h\equiv 1\ (\mathrm{mod}\ m).$

$h<\varphi(m),$ m

何

$$h=\varphi(m)=\varphi(2^\alpha)\varphi(p_1^{\alpha_1})\cdots\varphi(p_k^{\alpha_k}).$$

现在讨论何时 $h=\varphi(m)=\varphi(2^\alpha)\varphi(p_1^{\alpha_1})\cdots\varphi(p_k^{\alpha_k})$.

(a) $\alpha\geq 3$ $\tau=\dfrac{\varphi(2^\alpha)}{2}$. $h\leq\dfrac{\varphi(m)}{2}<\varphi(m)$.

(b) $k\geq 2$ $2|\varphi(p_1^{\alpha_1}),\quad 2|\varphi(p_2^{\alpha_2})$.

$[\varphi(p_1^{\alpha_1}),\varphi(p_2^{\alpha_2})]\leq\frac{1}{2}\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})<\varphi(p_1^{\alpha_1}p_2^{\alpha_2})$. $h<\varphi(m)$.

(c) $\alpha=2,\ k=1$ $\varphi(2^\alpha)=2,\quad 2|\varphi(p_1^{\alpha_1})$.

$$h=\varphi(p_1^{\alpha_1})<\varphi(2^n)\varphi(p_1^{\alpha_1})=\varphi(m).$$

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^α, $2p^\alpha$ 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.

8 $m > 1$, $\varphi(m)$ $q_1, \ldots, q_k$, g m

$$g^{\varphi(m)/q_i} \not\equiv 1 \pmod{m}, \quad i = 1, \ldots, k.$$

g m g m $\varphi(m)$.

$$0 < \varphi(m)/q_i < \varphi(m), \quad i = 1, \ldots, k.$$

§5.1 2, $g^{\varphi(m)/q_i} \not\equiv 1 \pmod{m}, \quad i = 1, \ldots, k.$

g m $e < \varphi(m)$. §5.1 1, $e|\varphi(m)$. q $q|\dfrac{\varphi(m)}{e}$.

$$\frac{\varphi(m)}{e} = qu, \qquad \frac{\varphi(m)}{q} = ue.$$

$g^{\varphi(m)/q} = (g^e)^u \equiv 1 \pmod{m}$.

定理 8 给出了一个找原根的方法.

1 41

$$\varphi(m) = \varphi(41) = 40 = 2^3 \cdot 5, \qquad \varphi(m)$$

$q_1 = 2,\ q_2 = 5.$ $\varphi(m)/q_1 = 20, \quad \varphi(m)/q_2 = 8.$

验 $g^{20},\ g^8$ m 1. 2, 3, . . . , 逐 验

$$2^8 \equiv 10,\ 2^{20} \equiv 1,\ 3^8 \equiv 1, \quad 4^8 \equiv 18,\ 4^{20} \equiv 1,$$
$$5^8 \equiv 18,\ 5^{20} \equiv 1,\ 6^8 \equiv 10,\ 6^{20} \equiv 40 \pmod{41},$$

6 41

因为 $(d, \varphi(m)) = 1$ 时, $\mathrm{ord}_m(g^d) = \mathrm{ord}_m(g)$, 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:

$$6^1 \equiv 6, \quad 6^3 \equiv 11, \quad 6^7 \equiv 29, \quad 6^9 \equiv 19, \quad 6^{11} \equiv 28,\ 6^{13} \equiv 24,\ 6^{17} \equiv 26,\ 6^{19} \equiv 34,$$
$$6^{21} \equiv 35,\ 6^{23} \equiv 30,\ 6^{27} \equiv 12,\ 6^{29} \equiv 22,\ 6^{31} \equiv 13,\ 6^{33} \equiv 17,\ 6^{37} \equiv 15,\ 6^{39} \equiv 7.$$

2 $m = 41^2 = 1681$, m

6 $p = 41$ 6 $6 + 41 = 47$

$41^2 = 1681$

$6^{40} \equiv 143 \equiv 1 + 41 \cdot 3 \pmod{41^2}$, $47^{40} \equiv 1518 \equiv 1 + 41 \cdot 37 \pmod{41^2}$.

$6^{40} \not\equiv 1 \pmod{41^2}$, $47^{40} \not\equiv 1 \pmod{41^2}$.

3 6 47 $m = 41^2 = 1681$

41^{α}

$(d, \varphi(m)) = 1$ $\mathrm{ord}_m(g^d) = \mathrm{ord}_m(g)$, d 遍历

$\varphi(41^2) = 1640$ 6^d 遍历 41^2

3 $m = 2 \cdot 41^2 = 3362$, m

3 2, $6 + 41^2 = 1687$ 47

$2 \cdot 41^2 = 3362$

4 43

$$m = 43, \qquad \varphi(m) = \varphi(43) = 2 \cdot 3 \cdot 7, \quad q_1 = 2,\ q_2 = 3,\ q_3 = 7.$$

$$\varphi(m)/q_1 = 21, \quad \varphi(m)/q_2 = 14, \quad \varphi(m)/q_3 = 6.$$

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：

$$2^2 \equiv 4, \quad 2^4 \equiv 16, \qquad 2^6 \equiv 64 \equiv 21, \qquad 2^7 \equiv 21 \cdot 2 \equiv -1,$$
$$2^{14} \equiv 1, \quad 3^2 \equiv 9, \qquad 3^4 \equiv 81 \equiv -5, \qquad 3^6 \equiv 9 \cdot (-5) \equiv -2,$$
$$3^7 \equiv -6,\ 3^{14} \equiv (-6)^2 \equiv 36,\ 3^{21} \equiv (-6) \cdot 36 \equiv -1 \pmod{43}.$$

3 43

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

$\varphi(\varphi(42)) = 12$ 3^d 43

$$3^1 \equiv 3, \quad 3^5 \equiv 28, \quad 3^{11} \equiv 30,\ 3^{13} \equiv 12,\ 3^{17} \equiv 26,\ 3^{19} \equiv 19, \quad 3^{23} \equiv 34,$$
$$3^{25} \equiv 5,\ 3^{29} \equiv 18,\ 3^{31} \equiv 33,\ 3^{37} \equiv 20,\ 3^{41} \equiv 29 \pmod{43}.$$

5 $m = 43^2 = 1849$, m

3 $p = 43$ 2, 3

$3 + 43 = 46$ $43^2 = 1849$

$$3^{42} \equiv 87 \equiv 1 + 43 \cdot 2 \pmod{43^2}, \quad 46^{40} \equiv 689 \equiv 1 + 43 \cdot 16 \pmod{43^2}.$$

$$3^{42} \not\equiv 1 \pmod{43^2}, \quad 46^{42} \not\equiv 1 \pmod{43^2}.$$

3 3 46 $m = 43^2 = 1849$

43^α

$m = p^\alpha$ $2p^\alpha$ m g

利 引 概念 研究 $x^n \equiv a \pmod m, \quad (a, m) = 1$

$a,\ (a, m) = 1,$ $r,\ 1 \le r \le \varphi(m),$

$g^r \equiv a \pmod m.$

1 m 1 g m a

m r

$$g^r \equiv a \pmod m, \quad 1 \le r \le \varphi(m)$$

r g 底 a m **标**,

$r = \mathrm{ind}_g a$ ($r = \mathrm{ind} a$).

1 5 17

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

$\text{ind}_5 1 = 16,\ \text{ind}_5 2 = 6,\ \ \text{ind}_5 3 = 13,\ \ \text{ind}_5 4 = 12,\ \text{ind}_5 5 = 14,\ \ \text{ind}_5 6 = 3,$
$\text{ind}_5 7 = 15,\ \text{ind}_5 8 = 2,\ \ \text{ind}_5 9 = 10,\ \ \text{ind}_5 10 = 7,\ \text{ind}_5 11 = 11,\ \text{ind}_5 12 = 9,$
$\text{ind}_5 13 = 4,\ \text{ind}_5 14 = 5,\ \text{ind}_5 15 = 14,\ \text{ind}_5 16 = 8.$

2 g $(a,m)=1$. r $g^r \equiv a \pmod{m}$

r $r \equiv \mathrm{ind}_g a \pmod{\varphi(m)}$.

$(a,m)=1$, $g^r \equiv a \equiv g^{\mathrm{ind}_g a} \pmod{m}$.

$g^{r-\mathrm{ind}_g a} \equiv 1 \pmod{m}$.

g m $\varphi(m)$, $\varphi(m) \mid r - \mathrm{ind}_g a$.

$$r \equiv \mathrm{ind}_g a \pmod{\varphi(m)}.$$

g $(a,m)=1$. $\mathrm{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$.

$g^0 \equiv 1 \pmod{m}$, 2,

$$\mathrm{ind}_g 1 \equiv 0 \pmod{\varphi(m)}.$$

3 m 1 g m r

$1 \leq r \leq \varphi(m)$. g m 相 r

m

4 m 1 g m

$a_1, \ldots, a_n$ m n

$$\operatorname{ind}_g(a_1 \cdots a_n) \equiv \operatorname{ind}_g(a_1) + \cdots + \operatorname{ind}_g(a_n) \pmod{\varphi(m)}.$$

$$\operatorname{ind}_g(a^n) \equiv n \operatorname{ind}_g(a) \pmod{\varphi(m)}.$$

例 2 作模 41 的指标表.

解 已知 6 是模 41 的原根，直接计算 $g^r \pmod m$:

$6^{40} \equiv 1,\quad 6^1 \equiv 6,\quad 6^2 \equiv 19,\quad 6^3 \equiv 11,\quad 6^4 \equiv 25,\quad 6^5 \equiv 27,\quad 6^6 \equiv 39,\quad 6^7 \equiv 29,$

$6^8 \equiv 10,\quad 6^9 \equiv 19,\quad 6^{10} \equiv 32,\ 6^{11} \equiv 28,\ 6^{12} \equiv 4,\quad 6^{13} \equiv 24,\ 6^{14} \equiv 21,\ 6^{15} \equiv 3,$

$6^{16} \equiv 18,\ 6^{17} \equiv 26,\ 6^{18} \equiv 33,\ 6^{19} \equiv 34,\ 6^{20} \equiv 40,\ 6^{21} \equiv 35,\ 6^{22} \equiv 5,\quad 6^{23} \equiv 30,$

$6^{24} \equiv 16,\ 6^{25} \equiv 14,\ 6^{26} \equiv 2,\quad 6^{27} \equiv 12,\ 6^{28} \equiv 31,\ 6^{29} \equiv 22,\ 6^{30} \equiv 9,\quad 6^{31} \equiv 13,$

$6^{32} \equiv 37,\ 6^{33} \equiv 17,\ 6^{34} \equiv 20,\ 6^{35} \equiv 38,\ 6^{36} \equiv 23,\ 6^{37} \equiv 15,\ 6^{38} \equiv 8,\quad 6^{39} \equiv 7.$

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									

3 $a = 28,\ 18$ 6 41

41 $g = 6$ 查 十 2

8 交叉 置 11 $\mathrm{ind}_6 28 = 11.$ 查 十

1 8 交叉 置 16 $\mathrm{ind}_6 18 = 16.$

什 呢？ r $g^r \equiv a \pmod{m}$ 很易 a r $g^r \equiv a \pmod{m}$ 常困难

2 m 1 a m n

$$x^n \equiv a \pmod{m} \qquad (1)$$

a m n **次剩余**; a m n **次非剩余**.

4 5 $x^5 \equiv 9 \pmod{41}$

41 9 0

9 30 $\mathrm{ind}_6 9 = 30.$ $x = 6^y \pmod{41}.$

変

$$6^{5y} \equiv 6^{30} \pmod{41}.$$

6 41 2

$5y \equiv 30 \pmod{40}$ $y \equiv 6 \pmod{8}.$

$y \equiv 6,\ 14,\ 22,\ 30,\ 38 \pmod{40}.$

$x \equiv 6^6 \equiv 39,\ x \equiv 6^{14} \equiv 21,\ x \equiv 6^{22} \equiv 5,$

$x \equiv 6^{30} \equiv 9,\ x \equiv 6^{38} \equiv 8,\quad x \equiv 6^{39} \equiv 7 \pmod{41}.$

5 g $(a,m)=1$. $x^n \equiv a \pmod m$ (2)

$(n,\varphi(m)) \mid \mathrm{ind}a,$

$(n,\varphi(m)).$

(2) $x \equiv x_0 \pmod m,$

负 $u,\ r$ $x_0 \equiv g^u, \quad a \equiv g^r \pmod m.$

(2) $g^{un} \equiv g^r \pmod m$ $un \equiv r \pmod{\varphi(m)}.$

$nX \equiv r \pmod{\varphi(m)}$ (3) $X \equiv u \pmod{\varphi(m)}.$

$(n,\varphi(m)) \mid \mathrm{ind}a.$

$(n,\varphi(m)) \mid \mathrm{ind}a,$ (3) $X \equiv u \pmod{\varphi(m)},$

$(n,\varphi(m)).$ (2) $x_0 \equiv g^u \pmod m,$ $(n,\varphi(m)).$

5 a m n

$a^{\varphi(m)/d} \equiv 1 \pmod{m}$, $d = (n, \varphi(m))$.

5 $x^n \equiv a \pmod{m}$

$nX \equiv r \pmod{\varphi(m)}$

$(n, \varphi(m)) \mid \mathrm{ind}a$, $\mathrm{ind}a \equiv 0 \pmod{d}$.

$\frac{\varphi(m)}{d}$, $\frac{\varphi(m)}{d}\mathrm{ind}a \equiv 0 \pmod{\varphi(m)}$.

$a^{\varphi(m)/d} \equiv 1 \pmod{m}$.

5 $x^8 \equiv 23 \pmod{41}$.

$d = (n, \varphi(m)) = (8, \varphi(41)) = (8, 40) = 8$, $\mathrm{ind}23 = 36$.

36 被 8

6 $x^{12} \equiv 37 \pmod{41}$.

$$d = (n, \varphi(m)) = (12, \varphi(41)) = (12, 40) = 4,$$
$$\text{ind}37 = 32.$$

$4 \mid 32$,

$$12 \ \text{ind}x \equiv \text{ind}37 \pmod{40}$$

$3 \ \text{ind}x \equiv 8 \pmod{10}$.

$$\text{ind}x \equiv 6,\ 16,\ 26,\ 36 \pmod{40}.$$

$$x \equiv 39,\ 18,\ 2,\ 23 \pmod{41}.$$

6 g $(a,m) = 1$. a m $e = \frac{\varphi(m)}{(\mathrm{ind}a,\varphi(m))}$.

a m $(\mathrm{ind}a, \varphi(m)) = 1$.

m g,

$$a = g^{\mathrm{ind}a} \pmod{m}.$$

§5.1 3, a

$$\mathrm{ord}(a) = \mathrm{ord}(g^{\mathrm{ind}a}) = \frac{\mathrm{ord}(g)}{(\mathrm{ord}(g), \mathrm{ind}a)} = \frac{\varphi(m)}{(\mathrm{ind}a, \varphi(m))}.$$

a m $\mathrm{ord}(a) = \varphi(m)$,

$$(\mathrm{ind}a, \varphi(m)) = 1.$$

7 g m m

e $\varphi(e)$. m

$\varphi(\varphi(m))$.

m g, §5.1 3, $a = g^d$

$$\operatorname{ord}(a) = \operatorname{ord}(g^d) = \frac{\operatorname{ord}(g)}{(\operatorname{ord}(g), d)} = \frac{\varphi(m)}{(d, \varphi(m))}.$$

a e $\dfrac{\varphi(m)}{(d, \varphi(m))} = e,$

$$(d, \varphi(m)) = \frac{\varphi(m)}{e}.$$

$d = d'\dfrac{\varphi(m)}{e}, \quad 0 \le d' < e.$ $(d', e) = 1.$ d'

$\varphi(e)$ $\varphi(m)$ $\varphi(\varphi(m))$.

$\varphi(\varphi(m))$.

第六章　素性检验

产　　产

Fermat　　n　　$b,\ (b,n)=1,$

$$b^{n-1}\equiv 1\ (\mathrm{mod}\ n).$$

$b,\ (b,n)=1$　　$b^{n-1}\not\equiv 1\ (\mathrm{mod}\ n),$

n　　合

1　　$2^{62}\equiv 2^{60}\cdot 2^2\equiv (2^6)^{10}\cdot 2^2\equiv 64^{10}\cdot 2^2\equiv 4\not\equiv 1\ (\mathrm{mod}\ 63),$

63　　合

2 $8^{62}\equiv (2^6)^{31}\equiv 1\ (\mathrm{mod}\ 63).$

1 n $b,\ (b,m)=1$

$b^{n-1}\equiv 1 \pmod{n}$ (1) n b **拟素** .

3 63 $b=8$ 拟

4 $341=11\cdot 31,\ 561=3\cdot 11\cdot 17,\ 645=3\cdot 5\cdot 43$

$b=2$ 拟

$$2^{340}\equiv 1 \pmod{340},\ 2^{560}\equiv 1 \pmod{561},\ 2^{644}\equiv 1 \pmod{645}.$$

1 $d,\ n$ d n, 2^d-1

2^n-1.

$d\,|n,$ q $n=dq.$

$$2^n-1=(2^d)^q-1=(2^d-1)((2^d)^{q-1}+(2^d)^{q-2}+\cdots+2^d+1).$$

$2^d-1\mid 2^n-1.$

1 穷多 2

(I) n 2 $m = 2^n - 1$

2 n 2

n $2^{n-1} \equiv 1 \pmod{n}$. n

$n = dq,\ 1 < d < n, 1 < q < n.$ $2^d - 1 \mid 2^n - 1.$

$m = 2^n - 1$ $2^{m-1} \equiv 1 \pmod{m}$.

$2^{n-1} \equiv 1 \pmod{n}$, $m - 1 = 2(2^{n-1} - 1) = kn.$

$2^n - 1 \mid 2^{m-1} - 1.$ $2^{m-1} \equiv 1 \pmod{m}$

$m = 2^n - 1$ 2

(II) n_0 2 $n_0 = 341$

2 $n_1 = 2^{n_0} - 1,\ n_2 = 2^{n_1} - 1,\ n_3 = 2^{n_2} - 1,\ \ldots.$

(I), 2

2 n

(i) n b b n 阶 $n-1$.

(ii) n b_1 b_2 n $b_1 b_2$

(iii) n b n b^{-1}

2 n (iv) $b,\ (b,n)=1,$ (1)

n 至少 半 (1)

(iv) $b_1,\ \ldots,\ b_s,\ b_{s+1},\ \ldots,\ b_{\varphi(n)}$

前 s (1) 后 $\varphi(n)-s$ (1)

$b,\ (b,n)=1,$ (1)

(ii) (iii), s n $bb_1,\ \ldots,\ bb_s$ (1)

$s \le \varphi(n)-s,$ $\varphi(n)-s \ge \dfrac{\varphi(n)}{2}.$ n

至少 半 (1)

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		

2 (iv) 告 $b,\ (b,n)=1,$

(1) n (1)

随机 $b,\ (b,n)=1,$ 50%

机会 n n 50% .

n

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, $\ldots,$ 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 $1 - \frac{1}{2^t}$.

Fermat 检

$n \geq 3$ 安 参 t.

1. $b,\ 2 \leq b \leq n-2$;
2. $r = b^{n-1} \pmod{n}$;
3. $r \neq 1$, n
4. 重复 t

2 n 称 **Carmichael**

$b,\ (b,n)=1,$

$$b^{n-1}\equiv 1 \pmod{n}$$

6 $561=3\cdot 11\cdot 17$ Carmichael

$(b,561)=1,$ $(b,3)=(b,11)=(b,17)=1.$ Fermat

$$b^2\equiv 1 \pmod 3,\quad b^{10}\equiv 1 \pmod{11},\quad b^{16}\equiv 1 \pmod{17}.$$

$$b^{560}\equiv (b^2)^{280}\equiv 1 \pmod 3,\quad b^{560}\equiv (b^{10})^{56}\equiv 1 \pmod{11},\quad b^{560}\equiv (b^{16})^{35}\equiv 1 \pmod{17}.$$

$$b^{560}\equiv 1 \pmod{561}.$$

3 n

(i) n 1 n Carmichael

(ii) $n = p_1 \cdots p_k$ n Carmichael

$$p_i - 1 \mid n - 1,\ 1 \le i \le k.$$

4 每 Carmichael

注 1. Carmichael

2. n 区间 $[2, n]$ Carmichael $\ge n^{2/7}$.

n $b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n}$

b

$b,\ (b,n)=1,$ $b^{(n-1)/2} \not\equiv \left(\frac{b}{n}\right) \pmod{n},$

n

1 $n=341,\ b=2.$ $2^{170} \equiv 1 \pmod{341}$

$\left(\frac{2}{341}\right) = (-1)^{(341^2-1)/8} = -1,$ $2^{170} \not\equiv \left(\frac{2}{341}\right) \pmod{341}.$ 341

1 n b n

n b $b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n},$

n b **Euler** .

2 $n = 1105,\ b = 2.$ $2^{552} \equiv 1 \pmod{1105}$

$\left(\frac{2}{1105}\right) = (-1)^{(1105^2-1)/8} = 1.$ $2^{552} \equiv \left(\frac{2}{1105}\right) \pmod{1105},$

1105 2 Euler

1 n b Euler n b

n 2 Euler $b^{(n-1)/2} \equiv \left(\frac{b}{n}\right) \pmod{n}.$

$$\left(\frac{b}{n}\right) = \pm 1 \pmod{n},$$

$$b^{n-1} \equiv (b^{(n-1)/2})^2 \equiv \left(\frac{b}{n}\right)^2 \equiv 1 \pmod{n},$$

n b

1 逆 Euler

341 2 2 Euler

Solovay-Stassen

$n \geq 3$ t.

1. $b,\ 2 \leq b \leq n-2$;
2. $r = b^{(n-1)/2} \pmod{n}$;
3. $r \neq 1$ $r \neq n-1$, n
4. Jacobi $s = \left(\frac{b}{n}\right)$;
5. $r \neq s$, n
6. t

n　　$n-1=2^s t,$

$$b^{n-1}-1=(b^{2^{s-1}t}+1)(b^{2^{s-2}t}+1)\cdots(b^t+1)(b^t-1).$$

$$b^{n-1}\equiv 1 \pmod{n},$$

$$b^t\equiv 1,\quad b^t\equiv -1,\quad b^{2t}\equiv -1,\ldots,\quad b^{2^{s-1}t}\equiv -1 \pmod{n}.$$

1　n　　$n-1=2^s t,$　　t

$(b,n)=1$.　　n　b　　$b^t\equiv 1 \pmod{n},$

$r,\ 0\le r<s$　　$b^{2^r t}\equiv -1 \pmod{n},$

n　　b　**强**　　.

1　　$n=2047=23\cdot 89$　　$b=2$　强

$$2^{2046/2}\equiv (2^{11})^{93}\equiv (2048)^{93}\equiv 1 \pmod{2046}.$$

1 2

2 n b n b Euler

3 n b, $1 \leq b \leq n-1$,
25%.

Miller-Rabin

$n \geq 3$ k, $n-1 = 2^s t$, t

1. b, $2 \leq b \leq n-2$; 2. $r_0 \equiv b^t \pmod{n}$;

3. a) $r_0 = 1$ $r_0 = n-1$, 通

回 1. 继续 b, $2 \leq b \leq n-2$;

b) $r_0 \neq 1$ $r_0 \neq n-1$, $r_1 \equiv r_0^2 \pmod{n}$;

4. a) $r_1 = n-1$, 通

回 1. 继续 b, $2 \leq b \leq n-2$;

b) $r_1 \neq n-1$, $r_2 \equiv r_1^2 \pmod{n}$; 如此继续下去,

s+2. a) $r_{s-1} = n-1$, 通

回 1. 继续 b, $2 \leq b \leq n-2$;

b) $r_{s-1} \neq n-1$, n

第七章　连分数

1. 连
2. 连
3. 连
4. 佳逼近
5. 连

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　　展开

$$\begin{aligned}
\sqrt{2} &= 1+(\sqrt{2}-1)\\
&= 1+\frac{1}{\sqrt{2}+1}\\
&= 1+\frac{1}{2+\dfrac{1}{\sqrt{2}+1}}\\
&= 1+\frac{1}{2+\dfrac{1}{2+\dfrac{1}{\sqrt{2}+1}}}\\
&= 1+\frac{1}{2+\dfrac{1}{2+\dfrac{1}{2+\dfrac{1}{\sqrt{2}+1}}}}\\
&= 1+\frac{1}{2+\dfrac{1}{2+\dfrac{1}{2+\dfrac{1}{2+\dfrac{1}{\sqrt{2}+1}}}}}.
\end{aligned}$$

$$1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2+\cfrac{1}{2}}}}=1+\cfrac{1}{2+\cfrac{1}{2+\cfrac{2}{5}}}=1+\cfrac{1}{2+\cfrac{5}{12}}$$

$$=1+\frac{12}{29}=\frac{41}{29}=1.413793103$$

$\sqrt{2}$ (10 制) 10 误差

i	a_i	P_i/Q_i	$\sqrt{2} - P_i/Q_i$
0	1	1/1	0.414213562
1	2	3/2	−0.085786438
2	2	7/5	0.014213562
3	2	17/12	−0.002453105
4	2	41/29	0.000420459

i	a_i	P_i/Q_i	$\sqrt{2} - P_i/Q_i$
5	2	99/70	−0.000072152
6	2	239/169	0.000012379
7	2	577/408	−0.000002124
8	2	1393/985	0.000000364
9	2	3363/2378	−0.000000063

1 $x_0, x_1, \ldots$ $x_i > 0, i \geq 1.$

$n \geq 0,$

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \ddots + \cfrac{1}{x_n}}}} \quad (1)$$

n **有限连分** , 值 $x_0, x_1, \ldots, x_n$

(1) n **有限简单连分** , 值

$$[x_0, x_1, \ldots, x_n]. \quad (2)$$

$0 \leq k \leq n,$ 限 $[x_0, x_1, \ldots, x_k]$ (3)

限 (1) 第 k **渐近分** . (2) 限

x_k 第 k **部分商**.

(1)((2)) $n \to \infty$

$$x_0 + \cfrac{1}{x_1 + \cfrac{1}{x_2 + \cfrac{1}{x_3 + \ddots}}} \qquad (4)$$

$[x_0, x_1, x_2, \ldots]$. (5) **无** . $x_0, x_1, \ldots$

(4) **无** . $k \geq 0$,

$[x_0, x_1, x_2, \ldots, x_k]$ (4) k .

(4) x_k k .

极 $\lim_{k\to\infty}[x_0, x_1, x_2, \ldots, x_k] = \theta$, (6)

(4)((5)) **收敛** θ (4)((5))

$[x_0, x_1, x_2, \ldots] = \theta$. **极** (6) (4)(

(5)) **发散**

a, b, c $b \neq 0.$ $f(x) = a + \dfrac{b}{c+x}$.

(i) $b > 0$ $f(x)$ $x > c$ ($x > c$) 调递减函

$c < x < x'$ ($x < x' < c$) $f(x) > f(x')$.

(ii) $b < 0$ $f(x)$ $x > c$ ($x > c$) 调递减函

$c < x < x'$ ($x < x' < c$) $f(x) < f(x')$.

$c < x < x'$ ($x < x' < c$),

$$f(x') - f(x) = (a + \frac{b}{c+x'}) - (a + \frac{b}{c+x}) = \frac{-b(x'-x)}{(c+x')(c+x)}.$$

$(c+x')(c+x) > 0,$ (i) $b > 0$ $f(x') < f(x).$ (ii)

$b < 0$ $f(x') > f(x).$

1 $x_0, x_1, \ldots$ $x_i > 0, i \geq 1.$

(i) 对任意整数 $n \geq 1,\ r \geq 1,$ 我们有

$$\begin{aligned} & [x_0, x_1, \ldots, x_{n-1}, x_n, \ldots, x_{n+r}] \\ = \ & [x_0, x_1, \ldots, x_{n-1}, [x_n, \ldots, x_{n+r}]\ ] \qquad (7) \\ = \ & [x_0, x_1, \ldots, x_{n-1}, x_n + 1/[x_{n+1}, \ldots, x_{n+r}]\ ]. \end{aligned}$$

特别地, $[x_0, x_1, \ldots, x_{n-1}, x_n, x_{n+1}] = [x_0, x_1, \ldots, x_{n-1}, x_n + 1/x_{n+1}]. \quad (8)$

(ii) 对任意实数 $\eta > 0$ 和整数 $n \geq 0,$

(a) 当 n 是奇数时, $[x_0, x_1, \ldots, x_{n-1}, x_n] > [x_0, x_1, \ldots, x_{n-1}, x_n + \eta,] \quad (9)$

(b) 当 n 是偶数时, $[x_0, x_1, \ldots, x_{n-1}, x_n] < [x_0, x_1, \ldots, x_{n-1}, x_n + \eta,] \quad (10)$

(iii) 对整数 $n \geq 0,$ 令 $\theta_n = [x_0, x_1, \ldots, x_{n-1}, x_n],$

(a) 对任意整数 $r \geq 1, \theta_{2n+1} > \theta_{2n+1+r},$ (b) 对任意整数 $r \geq 1, \theta_{2n} < \theta_{2n+r},$

(c) $\theta_1 > \theta_3 > \cdots \theta_{2n-1} > \cdots,$ (d) $\theta_0 < \theta_2 < \cdots \theta_{2n} < \cdots,$

(e) 对任意整数 $s \geq 1,\ t \geq 0, \theta_{2s-1} > \theta_{2t}.$

2 $x_0,\ x_1,\ x_2,\ \ldots \qquad\qquad x_j > 0,\ j \geq 1.$

$$P_{-2} = 0, \quad P_{-1} = 1, \quad P_n = x_n P_{n-1} + P_{n-2},\ n \geq 0, \quad (11)$$

$$Q_{-2} = 1, \quad Q_{-1} = 0, \quad Q_n = x_n Q_{n-1} + Q_{n-2},\ n \geq 0. \quad (12)$$

$$[x_0, x_1, \ldots, x_{n-1}, x_n] = \frac{P_n}{Q_n}, \quad n \geq 0, \quad (13)$$

$$P_n Q_{n-1} - P_{n-1} Q_n = (-1)^{n+1}, \quad n \geq -1, \quad (14)$$

$$P_n Q_{n-2} - P_{n-2} Q_n = (-1)^n x_n, \quad n \geq 0. \quad (15)$$

$$[x_0, x_1, \ldots, x_{n-1}, x_n] - [x_0, x_1, \ldots, x_{n-1}] \ = \ \frac{(-1)^{n+1}}{Q_{n-1} Q_n}, \quad n \geq 1, \quad (16)$$

$$[x_0, x_1, \ldots, x_{n-2}, x_{n-1}, x_n] - [x_0, x_1, \ldots, x_{n-2}] \ = \ \frac{(-1)^n x_n}{Q_{n-2} Q_n}, \quad n \geq 2. \quad (17)$$

商 渐

$\sqrt{2} = [1, 2, 2, 2, \ldots]$ 渐

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

$$1.412011 < \frac{P_6}{Q_6} = \frac{239}{169} < \sqrt{2} < \frac{P_7}{Q_7} = \frac{577}{408} < 1.412157.$$

α 公

3 $x_0,\ x_1,\ x_2,\ \ldots,\ x_n$ $x_j > 0,\ j \geq 1.$

$$\alpha = [x_0, x_1, x_2, \ldots, x_n], \quad \alpha_{k+1} = [x_{k+1}, \ldots, x_n] \quad (0 \leq k \leq n).$$

$$\alpha - \frac{P_k}{Q_k} = \frac{(-1)^k}{Q_k(\alpha_{k+1}Q_k + Q_{k-1})}.$$

1 (i) 2,

$$\alpha - \frac{P_k}{Q_k} = \frac{\alpha_{k+1}P_k + P_{k-1}}{\alpha_{k+1}Q_k + Q_{k-1}} - \frac{P_k}{Q_k}$$

$$= \frac{-(P_kQ_{k-1} - P_{k-1}Q_k)}{Q_k(\alpha_{k+1}Q_k + Q_{k-1})} = \frac{(-1)^k}{Q_k(\alpha_{k+1}Q_k + Q_{k-1})}.$$

x　　x

(i) 令 $a_0 = [x],\ x_0 = x - a_0.\ 0 \le x_0 < 1.$

(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 $\ldots\ldots,$ 得到 $a_k,\ x_k.$

(k+2) 如果 $x_k = 0,$ 则终止. 否则, 令 $a_{k+1} = [\frac{1}{x_k}],\ x_{k+1} = \frac{1}{x_k} - a_{k+1}.$　　$\ldots\ldots$

x

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \ldots \cfrac{}{} + \cfrac{1}{a_n + \ldots}}}.$$

$x = \dfrac{u_{-2}}{u_{-1}},\ u_{-1} \geq 1$ x

$[a_0, a_1, a_2, \ldots, a_n]$ $a_k,\ (0 \leq k \leq n)$

(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) $u_0 = a_2 u_1 + u_2, \quad 0 < u_2 = x_2 u_1 < u_1.$

$\ldots\ldots$

(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) $u_{n-2} = a_n u_{n-1} + u_n, \quad 0 = u_n = x_n u_{n-1} < u_{n-1}.$

$\{u_k\}_{k \geq -2}$ k 严格

$u_n = 0$ n $x_n = 0.$ $x = \dfrac{u_{-2}}{u_{-1}}$

$$x = [a_0, a_1, a_2, \ldots, a_n].$$

$a_n \geq 2$

$$x = [a_0, a_1, a_2, \ldots, a_n] = [a_0, a_1, a_2, \ldots, a_n - 1, 1].$$

种

答案

1 $[a_0, a_1, a_2, \ldots, a_n]$ $[b_0, b_1, b_2, \ldots, b_m]$

$a_n \geq 2,\ b_m \geq 2.$ $[a_0, a_1, a_2, \ldots, a_n] = [b_0, b_1, b_2, \ldots, b_m]$,

$n = m,\ a_i = b_i,\ i = 0, \ldots, n.$

2 $$x = \frac{u_0}{u_1}$$

$$x = [a_0, a_1, a_2, \ldots, a_n], \quad n \geq 1,\ a_n \geq 2$$

$$x = [a_0, a_1, a_2, \ldots, a_n - 1, 1], \quad n \geq 1,\ a_n \geq 2.$$

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
0	3	1265/2145	3	1
1	1	880/1265	4	1
2	1	385/880	7	2

i	a_i	x_i	P_i	Q_i
3	2	110/385	18	5
4	3	55/110	61	17
5	2	0	140	39

$$p = 107,\ q = 47.$$

i) $\dfrac{p}{q}$ ii) $\dfrac{p}{q}$

$$u_{-2} = p = 107,\ u_{-1} = q = 47.$$

$$\begin{aligned}
&\text{(i)} && 107 = 2 \cdot 47 + 13, && 0 < 13 = x_0 \cdot 47 < 47.\\
&\text{(ii)} && 47 = 3 \cdot 13 + 8, && 0 < 8 = x_1 \cdot 13 < 13.\\
&\text{(iii)} && 13 = 1 \cdot 8 + 5, && 0 < 5 = x_2 \cdot 8 < 8.\\
&\text{(iv)} && 8 = 1 \cdot 5 + 3, && 0 < 3 = x_3 \cdot 5 < 5.\\
&\text{(v)} && 5 = 1 \cdot 3 + 2, && 0 < 2 = x_4 \cdot 3 < 3.\\
&\text{(vi)} && 3 = 1 \cdot 2 + 1, && 0 < 1 = x_5 \cdot 2 < 2.\\
&\text{(vii)} && 2 = 2 \cdot 1 + 0, && 0 = x_6 \cdot 1 < 1.
\end{aligned}$$

i)

(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) $a_5 = [2/1] = 2, \quad x_6 = 1/x_5 - a_6 = 0.$

$$\frac{p}{q} = [2, 3, 1, 1, 1, 1, 2] \ .$$

ii)

i	a_i	x_i	P_i	Q_i
-2			0	1
-1			1	0
0	2	$13/47$	2	1
1	3	$8/13$	7	3
2	1	$5/8$	9	4
3	1	$3/5$	16	7
4	1	$2/3$	25	11
5	1	$1/2$	41	18
6	2	0	107	47

$$\frac{P_0}{Q_0} = 2, \quad \frac{P_1}{Q_1} = \frac{7}{3}, \quad \frac{P_2}{Q_2} = \frac{9}{4}, \quad \frac{P_3}{Q_3} = \frac{16}{7}, \quad \frac{P_4}{Q_4} = \frac{25}{11}, \quad \frac{P_5}{Q_6} = \frac{41}{18}, \quad \frac{P_6}{Q_6} = \frac{107}{47}.$$

2 $\alpha = (\sqrt{5}+1)/2$ 各

$$
\begin{aligned}
(\sqrt{5}+1)/2 &= 1 + (\sqrt{5}-1)/2 = 1 + \frac{1}{(\sqrt{5}+1)/2} \\
&= 1 + \frac{1}{1 + \dfrac{1}{(\sqrt{5}+1)/2}} \\
&= 1 + \frac{1}{1 + \dfrac{1}{1 + \dfrac{1}{(\sqrt{5}+1)/2}}} \\
&= 1 + \frac{1}{1 + \dfrac{1}{1 + \dfrac{1}{1 + \dfrac{1}{(\sqrt{5}+1)/2}}}}.
\end{aligned}
$$

i	a_i	x_i	P_i	Q_i
0	1	$(\sqrt{5}-1)/2$	1	1
1	1	$(\sqrt{5}-1)/2$	2	1
2	1	$(\sqrt{5}-1)/2$	3	2
3	1	$(\sqrt{5}-1)/2$	5	3
4	1	$(\sqrt{5}-1)/2$	8	5
5	1	$(\sqrt{5}-1)/2$	13	8
6	1	$(\sqrt{5}-1)/2$	21	13
7	1	$(\sqrt{5}-1)/2$	34	21
8	1	$(\sqrt{5}-1)/2$	55	34
9	1	$(\sqrt{5}-1)/2$	89	55

i	a_i	x_i	P_i	Q_i
10	1	$(\sqrt{5}-1)/2$	144	89
11	1	$(\sqrt{5}-1)/2$	233	144
12	1	$(\sqrt{5}-1)/2$	377	233
13	1	$(\sqrt{5}-1)/2$	610	377
14	1	$(\sqrt{5}-1)/2$	987	610
15	1	$(\sqrt{5}-1)/2$	1597	987
16	1	$(\sqrt{5}-1)/2$	2584	1597
17	1	$(\sqrt{5}-1)/2$	4181	2584
18	1	$(\sqrt{5}-1)/2$	6765	4181
19	1	$(\sqrt{5}-1)/2$	10946	6765

3 $[a_0, a_1, a_2, \ldots]$,

θ, $\lim_{n\to+\infty}[a_0, a_1, a_2, \ldots, a_n] = \theta$.

$n \geq 0$, $\theta_n = [a_0, a_1, a_2, \ldots, a_n]$. θ_n

§7.1 1, $\theta_1 > \theta_3 > \cdots \theta_{2n-1} > \cdots > \theta_0$,

$\theta_0 < \theta_2 < \cdots < \theta_{2n} < \cdots < \theta_1$.

$\{\theta_{2n-1}\}_{n\geq 1}$ 界 θ_0

$\lim_{n\to+\infty} \theta_{2n-1} = \theta'$.

$\{\theta_{2n}\}_{n\geq 0}$ 增 界 θ_1

$\lim_{n\to+\infty} \theta_{2n} = \theta''$.

$\theta_0 < \theta_2 < \cdots < \theta_{2n} < \cdots < \theta' \leq \theta'' < \cdots < \theta_{2n-1} < \cdots < \theta_1$.

§7.1 2, $n \geq 1$, $|\theta'' - \theta'| \leq |\theta_n - \theta_{n-1}| = \frac{1}{Q_{n-1}Q_n}$. $\theta' = \theta'' = \theta$.

4 $\theta > 1$ $\frac{P_n}{Q_n}$. $n \geq 1$,

$$|P_n^2 - \theta^2 Q_n^2| < 2\theta.$$

3 θ 介 $\frac{P_n}{Q_n}$ $\frac{P_{n+1}}{Q_{n+1}}$.

§7.1 2,

$$|P_n^2 - \theta^2 Q_n^2| = Q_n^2|\theta - \frac{P_n}{Q_n}||\theta + \frac{P_n}{Q_n}| < Q_n^2 \frac{1}{Q_n Q_{n+1}}(\theta + (\theta + \frac{1}{Q_n Q_{n+1}})).$$

$$2\theta(\frac{Q_n}{Q_{n+1}} + \frac{1}{2\theta Q_{n+1}^2}) - 2\theta < 2\theta \frac{Q_n + 1}{Q_{n+1}} - 2\theta \leq 2\theta \frac{Q_{n+1}}{Q_{n+1}} - 2\theta = 0,$$

θ $[a_0, a_1, a_2, \ldots]$. $m \geq 0$, m, $k \geq 1$, $n \geq m$,

$$a_{n+k} = a_k, \quad (1)$$

θ **循环** , **循环** . θ

$$\theta = [a_0, a_1, \ldots, a_{m-1}, \overline{a_m, \ldots, a_{m+k-1}}].$$

1 $\sqrt{2} = [1, 2, 2, \ldots] = [1, \overline{2}]$

$m = 0$, (1) θ **纯循环** ,
纯循环 .

2 $\dfrac{\sqrt{5}+1}{2} = [1, 1, 1, \ldots] = [\overline{1}]$ 纯

1 θ θ

$\theta = [\overline{a_0, \ldots, a_{k-1}}]$ §7.1 2,

$$\theta = [a_0, a_1, \ldots, a_{k-1}, \theta] = \frac{P_k}{Q_k} = \frac{\theta P_{k-1} + P_{k-2}}{\theta Q_{k-1} + Q_{k-2}},$$

$P_{k-2},\ P_{k-1},\ Q_{k-2},\ Q_{k-2}$

$$Q_{k-1}\theta^2 + (-P_{k-1} + Q_{k-2})\theta - P_{k-2} = 0.$$

θ

$$\theta = [a_0, a_1, \ldots, a_{m-1}, \overline{a_m, \ldots, a_{m+k-1}}]$$

$\theta_0 = [\overline{a_m, \ldots, a_{m+k-1}}]$ §7.1 2,

$$\theta = [a_0, a_1, \ldots, a_{k-1}, \theta_0] = \frac{P_k}{Q_k} = \frac{\theta_0 P_{k-1} + P_{k-2}}{\theta_0 Q_{k-1} + Q_{k-2}},$$

$P_{k-2},\ P_{k-1},\ Q_{k-2},\ Q_{k-2}$ θ

2 θ θ

效 描

1 θ $\frac{p}{q},\ (q>0)$ θ

$\frac{p'}{q'},\ 0<q'\le q,$

$$\left|\theta-\frac{p}{q}\right|<\left|\theta-\frac{p'}{q'}\right|. \qquad (1)$$

母 $q'\le q$ $\frac{p'}{q'}$ $\frac{p}{q}$ 距离 θ

$\frac{p}{q}$.

θ θ

1 θ $\dfrac{P_n}{Q_n},\ (n \geq 1)$ θ n

$p,\ q,\ (q > 0)$

$$|q\theta - p| < |Q_n\theta - P_n| \qquad (2)$$

$q \geq Q_{n+1}$.

2 θ θ $\dfrac{P_n}{Q_n},\ (n \geq 1),$

θ n $\dfrac{p}{q} \neq \dfrac{P_n}{Q_n},\ 0 < q \leq Q_n,$

$$\left|\theta - \frac{P_n}{Q_n}\right| < \left|\theta - \frac{p}{q}\right|. \qquad (4)$$

子

见

识　抽象

态、

态

1 S 空集 $S \times S$ S 映射 S **结合法** **运算**; 映射 (a, b) 像 a b **乘积**, $a \otimes b$ $a \cdot b$ $a * b$ ab, **乘法**.

加法, (a, b) 像 a b **和**, $a \oplus b$ $a + b$.

始终 S 空集

$a,\ b,\ c,$ $(ab)c = a(bc),$ **结合律**.

2 S S S **半群**.

$a,\ b,$ $ba = ab,$ **交换律**.

S e $ea = ae = a$ S a e S **位元**.

S 加 e S **零元**, 0.

1 : S e

e e' $e' = ee' = e.$

a S S a' $aa' = a'a = e,$

a S **逆** , a' a **逆** , $a^{-1}.$

a' a $-a.$

2 : S S

$a,$ a'

a' a'' a $aa' = a'a = e, \quad aa'' = a''a = e.$

a' a'' a

$$a' = a'e = a'(aa'') = (a'a)a'' = ea'' = a''.$$

a a'

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　　$\mathbf{N} = \{1, 2, \ldots, n, \ldots\}$

于通常　义下　　但没　零　和逆　;

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　　$\mathbf{Z} = \{\ldots, -n, \ldots, -2, -1, 0, 1, 2, \ldots, n, \ldots\}$

于通常　义下　　和零　0, 并且每

a　负　$-a$. 因此　$\mathbf{Z}$

零整　　$\mathbf{Z}^* = \mathbf{Z} \setminus \{0\}$　于通常　义下

和单位 1, 但不　每　　a　　逆　　因此 $\mathbf{Z}^*$ 不

3 理 $\mathbf{Q}$ $0,$

a $-a,$ $\mathbf{Q}$

理 $\mathbf{Q}^* = \mathbf{Q} \setminus \{0\}$

$1,$ a $a^{-1} = \frac{1}{a},$ $\mathbf{Q}^*$

类似 实 $\mathbf{R}$ 复 $\mathbf{C}$ 而 实 $\mathbf{R}^* = \mathbf{R} \setminus \{0\}$ 复 $\mathbf{C}^* = \mathbf{C} \setminus \{0\}$

4 D 平方 $\mathbf{Z}(\sqrt{D}) = \{a + b\sqrt{D} \mid a, b \in \mathbf{Z}\}$

运算 $(a + b\sqrt{D}) \oplus (c + d\sqrt{D}) = (a + c) + (b + d)\sqrt{D}$ 构成

运算 $(a + b\sqrt{D}) \otimes (c + d\sqrt{D}) = (ac + bdD) + (bc + ad)\sqrt{D}$ 构成

5 n 正 $\mathbf{Z}/n\mathbf{Z} = \{0, 1, 2, \ldots, n-1\}$.

证明 $\mathbf{Z}/n\mathbf{Z}$ $a \oplus b = (a + b \pmod{n})$

其中 $a \pmod{n}$ 是整数 a 模 n 的最小非负剩余.

0, a $n - a$. $n = 6$

$a \setminus x$	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

6 p $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$. $\mathbf{F}_p^* = \mathbf{F}_p \setminus \{0\}$.

$\mathbf{F}_p^*$ $a \otimes b = (a \cdot b \pmod{p})$

1, a $(a^{-1} \pmod{p})$. $p = 7$

$a \setminus x$	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

7 n $\mathbf{Z}/n\mathbf{Z} \setminus \{0\}$

$a \otimes b = (a \cdot b \pmod{n})$

1. n 真 d $d' \in$ $\mathbf{Z}/n\mathbf{Z} \setminus \{0\}$, $d \otimes d' = (d \cdot d' \pmod{n}) \neq 1$. $n = 6$

$a \setminus x$	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

8 n $(\mathbf{Z}/n\mathbf{Z})^* = \{a \mid a \in \mathbf{Z}/n\mathbf{Z},\ (a,n) = 1\}$.

$(\mathbf{Z}/n\mathbf{Z})^*$ $a \otimes b = (a \cdot b \pmod{n})$

1, a $(a^{-1} \pmod{n})$. $n = 15$

$a \setminus x$	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

9. 域 $\mathbf{K}$ 全体 n 级矩阵组

$$M_n(\mathbf{K}) = \{(a_{ij})_{1\leq i\leq n, 1\leq j\leq n} \,|a_{ij} \in \mathbf{K},\ 1 \leq i \leq n, 1 \leq j \leq n\}.$$

$A = (a_{ij}),\ B = (b_{ij}),\ C = (c_{ij}), \in M_n(\mathbf{K})$. 我们定

$$A + B = C, \quad \text{其} \quad c_{ij} = a_{ij} + b_{ij},\ 1 \leq i \leq n, 1 \leq j \leq n.$$

$M_n(\mathbf{K})$

$$\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} + \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} = \begin{pmatrix} a_{11} + b_{11} & a_{12} + b_{12} \\ a_{21} + b_{21} & a_{22} + b_{22} \end{pmatrix}$$

$$\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \qquad \begin{pmatrix} -a_{11} & -a_{12} \\ -a_{21} & -a_{22} \end{pmatrix}$$

9' $A=(a_{ij}),\ B=(b_{ij}),\ C=(c_{ij}),\in M_n(\mathbf{K}).$

$A\cdot B=C,\qquad c_{ij}=\sum\limits_{k=1}^{n}a_{ik}b_{kj},\ 1\le i\le n, 1\le j\le n.$

$M_n(\mathbf{K})\setminus\{0\}$

$$\begin{pmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{pmatrix}\cdot\begin{pmatrix}b_{11} & b_{12}\\ b_{21} & b_{22}\end{pmatrix}=\begin{pmatrix}a_{11}b_{11}+a_{12}b_{21} & a_{11}b_{12}+a_{12}b_{22}\\ a_{21}b_{11}+a_{22}b_{21} & a_{21}b_{12}+a_{22}b_{22}\end{pmatrix}$$

$$\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix},\quad \begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}\cdot\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix}=\begin{pmatrix}0\cdot 0+1\cdot 0 & 0\cdot 1+1\cdot 0\\ 0\cdot 0+0\cdot 0 & 0\cdot 1+0\cdot 0\end{pmatrix}=\begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$$

可 A (A' $AA'=A'A=I_n$)

$GL_n(P)$, 称 n **一般线** ;

$GL_n(P)$ 行列式 1 也

这 $SL_n(p)$, 称 **特殊线** .

10 S G S 到 身 所 应
映射 f $f, g \in G,$ f g 映射 $g \circ f$

$$x \in S,\ g \circ f(x) = g(f(x)).$$

G 映射 **对称** .

恒等映射 G S **置** .

S n G n **对称** , S_n.

多个　素的运算　$a_1, a_2, \ldots, a_{n-1}, a_n$　G　n

归纳　n　积

$$a_1 a_2 \cdots a_{n-1} a_n = (a_1 a_2 \cdots a_{n-1}) a_n.$$

G　归纳　n

$$a_1 + a_2 + \cdots + a_{n-1} + a_n = (a_1 + a_2 + \cdots + a_{n-1}) + a_n.$$

质 3： $a_1, \ldots, a_n$ G $n \geq 2$

$1 \leq i_1 < \ldots < i_k < n,$

$$(a_1 \cdots a_{i_1}) \cdots (a_{i_k+1} \cdots a_n) = a_1 a_2 \cdots a_{n-1} a_n.$$

质 4： $a_1, a_2, \ldots, a_{n-1}, a_n$ G $n \geq 2$

$1, 2, \ldots, n$ 排 $i_1, i_2, \ldots, i_n,$

$$a_{i_1} a_{i_2} \cdots a_{i_n} = a_1 a_2 \cdots a_n.$$

n $a_1 = a_2 = \cdots = a_n = a,$ $a_1 a_2 \cdots a_n = a^n,$

之 a n 次幂 $a^0 = e$ $a^{-n} = (a^{-1})^n$

a^{-1} n 次幂

质 5: 设 $a \in G$, 则对任意 $m,\ n \in \mathbf{Z},$

$$a^m a^n = a^{m+n}, \quad (a^m)^n = a^{mn}.$$

理 1　$G \neq \emptyset$　　G　　程 $ax = b, \quad ya = b$

G　　解　反过来　　上述　程　G　　解

G

4　H　　G　　子　　G

H　　H　　G　**子**　,　　$H \leq G.$

$H = \{e\}$　　$H = G$　　G　子　　G　**平凡子**　.

G　子　H　　G　**真子**　,　　H　　G　　凡子

11　n　　$n\mathbf{Z} = \{nk \mid k \in \mathbf{Z}\}$　　$\mathbf{Z}$　子

11' 例 10'　　$H_1,\ H_2,\ H_3,\ H_4$　　S_3　　子

2 H G H G 充要条件 $a,\ b \in H,\quad ab^{-1} \in H.$

证 必要性 显 充分性

G 以 G $a.$ 根据假 $e = aa^{-1} \in H.$ H $e \in H$ 及 $a,$ 再 用假 $a^{-1} = ea^{-1} \in H,$ H a H H G 毕

3 G $\{H_i\}_{i\in I}$ G 族

$$\bigcap_{i\in I} H_i = H_1 \cap H_2 \cap \cdots \cap H_n \cap \cdots$$

G

$a,\ b \in \cap_{i\in I} H_i,$

$a,\ b \in H_i, \qquad i \in I.$

H_i G 2, $ab^{-1} \in H_i,\ i \in I.$ 进

$$ab^{-1} \in \bigcap_{i\in I} H_i.$$

2, $\cap_{i\in I} H_i$ G

5 G X G $\{H_i\}_{i\in I}$ G 包含 X

$$\bigcap_{i\in I} H_i$$

G 由 X **生成** . $< X >$.

X $< X >$ **生成** .

$X = \{a_1, \ldots, a_n\}$, $< X >$ $< a_1, \ldots, a_n >$.

$G =< a_1, \ldots, a_n >$, G **生成** .

$G =< a >$, G a 生 **循环** .

4 G X G X

$$< X >= \{a_1^{n_1} \cdots a_t^{n_t} \mid t \in \mathbf{N},\ a_i \in G,\ n_i \in \mathbf{Z},\ 1 \leq i \leq t\}.$$

$a \in G$,

$$< a >= \{a^n \mid n \in \mathbf{Z}\}.$$

12 $G =< g >= \{g^r \mid g^r \neq 1,\ 1 \leq r < n,\ g^n = 1\}$. G n 阶循环 $< g^d >= \{g^{dk} \mid k \in \mathbf{Z}\}$ G

1　$G,\ G'$　两　f　G　G'

$a,\ b \in G,$　$f(ab) = f(a)f(b),$

f　G　G'　**同态**.

G　G'　同态　$\mathrm{Hom}(G, G')$.

f　f　**同态**;　f

f　**满同态**;　f　f　**同构**.

$G = G'$　同态 f　**自同态**, 同　f　**自同构**.

2　$G,\ G'$　两　G 与 G' **同构**,

G　G'　同　$G \cong G'$.

1 f G G'

(i) $f(e) = e'$, (ii) $a \in G$, $f(a^{-1}) = f(a)^{-1}$.

(iii) $\ker f = \{a \mid a \in G,\ f(a) = e'\}$ G

f $\ker f = \{e\}$.

2 f G G'

(iv) $f(G) = \{f(a) \mid a \in G\}$ G'

f $f(G) = G'$.

(v) H' G' $f^{-1}(H') = \{a \in G \mid f(a) \in H'\}$ G

$\ker f$ f **核** , $f(G)$ **象** .

1 $\mathbf{Z}$ $G =< g >= \{g^n \mid n \in \mathbf{Z}\}$ $f : n \longmapsto g^n$ $\mathbf{Z}$ $< g >$

$$a, b \in \mathbf{Z}, \qquad f(a+b) = g^{a+b} = g^a g^b = f(a)f(b).$$

2 $\mathbf{Z}$ $\mathbf{R}^* = \mathbf{R} \setminus \{0\}$ $f : a \longmapsto e^a$ $\mathbf{R}$ $\mathbf{R}^*$

3 $\mathbf{Z}$ $\mathbf{Z}/n\mathbf{Z}$ $f : n \longmapsto g^n$

4 $\mathbf{Z}$ $G = \{\theta^k | \theta = e^{\frac{2\pi i}{n}},\ k \in \mathbf{Z}\}$ $f : k \longmapsto \theta^k$

5 $\mathbf{Z}/n\mathbf{Z}$ $G = \{\theta^k | \theta = e^{\frac{2\pi i}{n}},\ k = 0,\ 1,\ \ldots, n-1\}$ $f : k + n\mathbf{Z} \longmapsto \theta^k$

6 a G

$$f : b \longmapsto aba^{-1}$$

G 事

$$f(bc) = a(bc)a^{-1} = (aba^{-1})(aca^{-1}) = f(a)f(b).$$

1 H G a G

$aH = \{ah | h \in H\}$ ($Ha = \{ha | h \in H\}$) G H

左 (右)**陪集**. aH (Ha) aH (Ha) 代表 $aH = Ha$, aH G H **陪集**

1 $n > 1$ $H = n\mathbf{Z}$ $\mathbf{Z}$

$$a + n\mathbf{Z} = \{a + nk \mid k \in \mathbf{Z}\}$$

就 $n\mathbf{Z}$ 陪 陪 就 模 n 剩余

1 H G

(i) $a \in G$, $aH = \{c \mid c \in G,\ c^{-1}a \in H\}$ ($Ha = \{c \mid c \in G,\ ac^{-1} \in H\}$);

(ii) $a,\ b \in G$, $aH = bH$ $b^{-1}a \in H$ ($Ha = Hb$ $ab^{-1} \in H$);

(iii) $a,\ b \in G$, $aH \cap bH = \emptyset$ $b^{-1}a \notin H$ ($Ha \cap Hb = \emptyset$ $ab^{-1} \notin H$);

(iv) $a \in H$, $aH = H = Ha$.

推论 H G G 示 相 ( )

2 H G H G ( )

新 $\{aH \mid a \in G\}$, H G **商** , G/H.

G/H ( ) H G **指标** ,

$[G : H]$.

2 $H \leq G$, $|G| = [G : H]|H|$.

更 步 K, $H \leq G$, $K \leq H$, $[G : K] = [G : H][H : K]$.

指标 第三 指标

(Lagrange). H G H $|G|$

6 N G 价

(i) $a \in G,\quad aN = Na;$

(ii) $a \in G,\quad aNa^{-1} = N.$

(iii) $a \in G,\quad aNa^{-1} \subset N,\quad aNa^{-1} = \{ana^{-1} | n \in N\}.$

易知 (i) 蕴 (ii) (ii) 蕴 (iii) 现从 (iii) 推出 (i). $a \in G,\ n \in N,\quad ana^{-1} \in aNa^{-1} \subset N,$ $ana^{-1} = n',\ n' \in N.$ $an = n'a \in Na$ $aN \subset Na.$ $a^{-1}N \subset Na^{-1}$ $Na \subset aN.$ 故 $aN = Na.$ 立

3 N G N G **正规** ,

它 6 $N \triangleleft G.$

7 $N \triangleleft G$, $G/N = \{aN \mid a \in G\}$.

$(aN)(bN) = (ab)N$, G/H

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/H 构成一个群. 证毕.

7 G 规 H . G

G/N $(a+N)+(b+N) = (a+b)+N.$

8 f G G' f 核 $\ker(f)$ G

N G G G/N

$s : a \longmapsto aN$ 核 N

$a \in G,\ b \in \ker f,$ $f(aba^{-1}) = f(a)f(b)f(a^{-1}) =$

$f(a)e'f(a)^{-1} = e'.$ 说 $aba^{-1} \in \ker f.$ 6, $\ker(f)$ G

N G G G/N s

$$s(ab) = (ab)N = (aN)(bN) = s(a)s(b),$$

$s(a) = N$ $a \in N.$ s 核 N

$s : G \longrightarrow G/N$ G G/N **然** .

9 $f \in \mathrm{Hom}(G, G')$, 惟 $G/\ker(f)$ $f(G)$

$\overline{f} : a\ker(f) \longmapsto f(a)$ $f = i \circ \overline{f} \circ s,$ s G $G/\ker(f)$

i $f(G)$ G' 图

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ \mathrm{s}\downarrow & & \uparrow \mathrm{i} \\ G/\ker(f) & \xrightarrow{\overline{f}} & f(G) \end{array}$$

$\ker(f) \lhd G$, 商 $G/\ker(f).$

$\overline{f} : a\ker(f) \longmapsto f(a)$ $G/\ker(f)$ 像 $f(G)$

首先 $\overline{f}$ $G/\ker(f)$ $f(G)$

$a\ker(f),\ b\ker(f) \in G/\ker(f),$

$$\overline{f}((a\ker(f))(b\ker(f)) = \overline{f}((ab)\ker(f)) = f(ab) = f(a)f(b) = \overline{f}(a\ker(f))\overline{f}(b\ker(f)).$$

$\overline{f}$ $a\ker(f) \in \ker(\overline{f})$,

$\overline{f}(a\ker(f)) = f(a) = e'$. $a \in \ker(f)$ $a\ker(f) = \ker(f)$.

最后 $\overline{f}$ $c \in f(G)$, $a \in G$

$f(a) = c$. $\overline{f}(a\ker(f)) = f(a) = c$. $a\ker(f)$ c 源

$\overline{f}$ $f = i \circ \overline{f} \circ s$. $a \in G$,

$$i \circ \overline{f} \circ s(a) = i(\overline{f}(s(a))) = i(\overline{f}(a\ker(f))) = i(f(a)) = f(a).$$

$g : G/\ker(f) \longrightarrow f(G)$ $f = i \circ g \circ s$,

$a\ker(f) \in G/\ker(f)$,

$$g(a\ker(f)) = i(g(s(a))) = (i \circ g \circ s)(a) = f(a) = \overline{f}(a\ker(f)).$$

$g = \overline{f}$.

第九章　群的结构

1 $\mathbf{Z}$ H $H = \{0\}$ $H =< m >= m\mathbf{Z}$, m H 小 $H \neq < 0 >$, H 无

$H = \{0\}$, 论 $H \neq \{0\}$, $a \in H$. H $-a \in H$. H H 小 m. $H =< m >= m\mathbf{Z}$.

$a \in H$, 欧几里 除 q, r

$$a = qm + r, \quad 0 \leq r < m.$$

$r \neq 0$, $r = a - qm \in H$, m 小 矛盾

$r = 0$, $a = qm \in m\mathbf{Z}$. $H \subset m\mathbf{Z}$. $m\mathbf{Z} \subset H$.

$H = m\mathbf{Z}$.

2 $\mathbf{Z}$. m

$\mathbf{Z}/m\mathbf{Z}$.

$G =< a >= \{a^n \mid n \in \mathbf{Z}\}$. 考虑

$$f : \mathbf{Z} \longrightarrow G$$
$$n \longmapsto a^n$$

$f(n+m) = a^{n+m} = a^n a^m = f(n)f(m)$, f $\mathbf{Z}$ G

§8.3 9, G $\mathbf{Z}/\ker(f)$.

1, $\ker(f) =< 0 >$ $\ker(f) = m\mathbf{Z}$. 前者 者

m

1 G $a \in G$. $< a >$ a

$\mathrm{ord}(a)$.

3 G $a \in G$. a

(i) $a^k = e \Leftrightarrow k = 0$. (ii) a^k $(k \in \mathbf{Z})$

a $m > 0$,

(iii) m $a^m = e$ (iv) $a^k = e \Leftrightarrow m|k$.

(v) $a^r = a^k \Leftrightarrow r \equiv k \pmod{m}$. (vi) a^k $(k \in \mathbf{Z}/m\mathbf{Z})$

(vii) $< a >= \{a, a^2, a^{m-1}, a^m = e\}$ (viii) $\mathrm{ord}(a^d) = \dfrac{m}{(m,d)}$.

4

5 G G G

a a^{-1}. G m, a^k G 仅

$(k, m) = 1$.

引　1　G　$a, b \in G,$

若 $(\mathrm{ord}(a), \mathrm{ord}(b)) = 1,$

$$\mathrm{ord}(ab) = \mathrm{ord}(a)\mathrm{ord}(b).$$

引　2　G　$a, b \in G,$　$c \in G$

$$\mathrm{ord}(c) = [\mathrm{ord}(a), \mathrm{ord}(b)].$$

6　G　G　$a_1,\ a_2,\ \ldots,\ a_s$

各　$m_1,\ m_2,\ \ldots, m_s$　$m_i | m_{i+1},\ 1 \leq i \leq s-1,$

$$G =< a_1 >< a_2 > \cdots < a_s > .$$

G. X G X

线

$$n_1x_1 + n_2x_2 + \cdots + n_kx_k, \quad k \in \mathbf{N},\ n_i \in \mathbf{Z},\ x_i \in X$$

$$< x >= \{nx | n \in \mathbf{Z}\}.$$

G X G **基底**, X G

(i) $G =< X >$; (ii) X

$x_1, x_2, \ldots, x_k$ $\mathbf{Z}$ **关**,

$n_1, n_2, \ldots, n_k$ $n_1x_1 + n_2x_2 + \cdots + n_kx_k = 0.$

线 关 **关**,

$n_1, n_2, \ldots, n_k$ $x_1^{n_1}x_2^{n_2}\cdots x_k^{n_k} = e.$

$H_1, \ldots, H_k$ G k $H_1 + \cdots + H_k$

$H_1, \ldots, H_k$ **直和**, $(H_1 + \cdots + H_{i-1} + H_{i+1} + \cdots + H_k) \cap H_i = \{0\}$, $1 \leq i \leq k$. $H_1 \oplus \cdots \oplus H_k$.

$H_1 \cdots H_k$ $H_1, \ldots, H_k$ **直積**, $(H_1 \cdots H_{i-1} H_{i+1} \cdots H_k) \cap H_i = \{e\}$, $1 \leq i \leq k$. $H_1 \otimes \cdots \otimes H_k$.

1 G 基底 G

直

1 **由** .

2 基底

G 基底 G **秩**.

3 G 秩 $|X|$

象 X G

4 G 直

$m_1, \ldots, m_s$ $m_1|m_2, \ldots, m_{s-1}|m_s$.

研究 S_n. $S=\{1,\ 2,\ \ldots,\ n-1,\ n\}$, σ S 置 σ S

$$\sigma : S \longrightarrow S$$
$$k \longmapsto \sigma(k)=i_k$$

k σ i_k, 将 σ

$$\sigma=\begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n-1) & \sigma(n) \end{pmatrix}=\begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ i_1 & i_2 & \ldots & i_{n-1} & i_n \end{pmatrix}.$$

$$\sigma=\begin{pmatrix} n & n-1 & \ldots & 2 & 1 \\ i_n & i_{n-1} & \ldots & i_2 & i_1 \end{pmatrix}=\begin{pmatrix} j_1 & j_2 & \cdots & j_{n-1} & j_n \\ i_{j_1} & i_{j_2} & \cdots & i_{j_{n-1}} & i_{j_n} \end{pmatrix},$$

$j_1,\ j_2,\ \ldots,\ j_{n-1},\ j_n$ $1,\ 2,\ \ldots,\ n-1,\ n$

1 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 2 & 1 & 3 \end{pmatrix}$, $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 2 & 3 & 1 \end{pmatrix}$. 计 $\sigma\tau$, $\tau\sigma$, σ^{-1}.

$$\sigma \cdot \tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 2 & 3 & 1 \end{pmatrix}$$

$$= \begin{pmatrix} 5 & 6 & 4 & 2 & 3 & 1 \\ 1 & 3 & 2 & 5 & 4 & 6 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 4 & 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 5 & 4 & 6 \end{pmatrix}.$$

$$\tau \cdot \sigma = \begin{pmatrix} 6 & 5 & 4 & 2 & 1 & 3 \\ 1 & 3 & 2 & 6 & 5 & 4 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 3 & 2 & 6 & 5 & 4 \end{pmatrix}.$$

$$\sigma^{-1} = \begin{pmatrix} 6 & 5 & 4 & 2 & 1 & 3 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 4 & 6 & 3 & 2 & 1 \end{pmatrix}.$$

1 n S_n

$n!$.

仍 该

又 n $e = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ 1 & 2 & \dots & n-1 & n \end{pmatrix}$

$\sigma = \begin{pmatrix} 1 & 2 & \dots & n-1 & n \\ i_1 & i_2 & \dots & i_{n-1} & i_n \end{pmatrix}$ $\sigma^{-1} = \begin{pmatrix} i_1 & i_2 & \dots & i_{n-1} & i_n \\ 1 & 2 & \dots & n-1 & n \end{pmatrix}$.

S_n

$(1,\ 2,\ \dots,\ n-1,\ n)$ σ $(\sigma(1),\ \sigma(2),\ \dots,\ \sigma(n-1),\ \sigma(n)\xi)$ $(1,\ 2,\ \dots,\ n-1,\ n)$ 样 共 $n!$

S_n $n!$.

n σ $\{1,\ 2,\ \ldots,\ n-1,\ n\}$ 部
$\{i_1,\ i_2,\ \ldots,\ i_{k-1},\ i_k\}$ $\sigma(i_1) = i_2,\ \sigma(i_{k-1}) = i_k,\ \sigma(i_k) = i_1,$
保持 变 $k-$**轮** , 简 轮

$$\sigma = (i_1,\ i_2,\ \ldots,\ i_{k-1},\ i_k).$$

k 轮 长度 $k = 1$ 1- 轮 $k = 2$ 2-
轮 (i_1, i_2) .
轮 $\sigma = (i_1,\ i_2,\ \ldots,\ i_{k-1},\ i_k),\ \tau = (j_1,\ j_2,\ \ldots,\ j_{l-1},\ j_l)$
$k + l$

2 些

序 情况 达

σ $S=\{1,\ 2,\ \ldots,\ n-1,\ n\}$ S

取 $i_1^{(1)}$. $n+1$

$$i_1^{(1)},\ \sigma^1(i_1^{(1)}),\ \ldots,\ \sigma^n(i_1^{(1)})$$

落 n S $k\neq l$ $\sigma^k(i_1^{(1)})=\sigma^l(i_1^{(1)})$.

妨 $k>l$, $\sigma^{k-l}(i_1^{(1)})=i_1^{(1)}$.

取 $k_1\leq n$ $\sigma^{k_1}(i_1^{(1)})=i_1^{(1)}$ 令

$$i_2^{(1)}=\sigma^1(i_1^{(1)}),\ \ldots,\ i_{k_1}^{(1)}=\sigma^{k_1-1}(i_1^{(1)}).$$

$\sigma_1=(i_1^{(1)},\ i_2^{(1)},\ \ldots,\ i_{k_1}^{(1)})$ k_1-

$k_1=n$, $\sigma=\sigma_1$.

$k_1 < n,$ $S - \{i_1^{(1)},\ i_2^{(1)},\ \ldots,\ i_{k_1}^{(1)}\}$

$i_1^{(2)}.$ $k_2 \le n$ $\sigma^{k_2}(i_1^{(2)}) = i_1^{(2)}$

$$i_2^{(2)} = \sigma^1(i_1^{(2)}),\ \ldots,\ i_{k_2}^{(2)} = \sigma^{k_2-1}(i_1^{(2)}).$$

$\sigma_2 = (i_1^{(2)},\ i_2^{(2)},\ \ldots,\ i_{k_2}^{(1)})$ σ_1 k_2-

去 $\ldots,$ 找 $\sigma_1,\ \ldots,\ \sigma_{r-1}$ k_r- σ_r

$k_1 + k_2 + \cdots + k_r = n.$ $i \in S,$

$$\sigma_1\sigma_2\cdots\sigma_r(i) = \sigma(i),$$

2 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 2 & 4 & 3 \end{pmatrix} = (2,5,4)(1,6,3).$

$$\sigma = (i_1,\ i_2,\ \ldots,\ i_{k-1},\ i_k),$$

$$\sigma = (i_1,\ i_2,\ \ldots,\ i_{k-1},\ i_k) = (i_1, i_k)(i_1, i_{k-1}) \cdots (i_1, i_3)(i_1, i_2).$$

2 $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 1 & 2 & 4 & 3 \end{pmatrix} = (2,5,4)(1,6,3) = (2,4)(2,5)(1,3)(1,6).$

1 n $i_1,\ \ldots,\ i_k,\ \ldots,\ i_l,\ \ldots,\ i_n$

$(i_k,\ i_l)$ **序**, $k < l$ $i_k > i_l$.

序数, $[i_1,\ \ldots,\ i_n]$.

3 σ

奇偶 $[\sigma(1),\ \ldots,\ \sigma(n)]$ 奇偶

明 $\tau = (\sigma(k),\ \sigma(l)),$ $\sigma(1),\ \ldots,\ \sigma(k),\ \ldots,\ \sigma(l),\ \ldots,\ \sigma(n)$

$$\sigma(1),\ \ldots,\ \sigma(l),\ \ldots,\ \sigma(k),\ \ldots,\ \sigma(n)$$

发 改

$$(\sigma(k),\ \sigma(k+1)),\ \ldots,\ (\sigma(k),\ \sigma(l)),\ (\sigma(k+1),\ \sigma(l)),\ \ldots,\ (\sigma(l-1),\ \sigma(l)),$$

2(l-k)+1 改 $[\sigma(1),\ldots,\sigma(n)]$ 奇偶

$\sigma = \tau_k \cdots \tau_1$ m $1,\ldots,n$ 经 m $\sigma(1),\ldots,\sigma(n)$. $[\sigma(1),\ldots,\sigma(n)]$ 奇偶 $[1,\ldots,n] + m = m$ 奇偶

2 σ **偶** ,

σ **奇** ,

A_n n

4 A_n $n!/2$.

A_n

n

$\tau A_n = \{\tau\sigma \mid \sigma \in A_n\}$, τ 给

τ, $S_n = A_n \cup \tau A_n$ $|S_n| =$

$|A_n| + |\tau A_n| = 2A_n.$ $|A_n| = n!/2.$

A_n **错** .

n n .

3 $\sigma = (1,\ 2,\ 3)$. $G =< \sigma >= \{e,\ (1,\ 2,\ 3),\ (1,\ 3,\ 2)\}$

3

4 $\sigma_1 = (1,\ 2,\ 3,\ 4),\ \sigma_2 = (1,\ 3,\ 2,\ 4)$. $G_1 =< \sigma_1 >= \{e,\ (1,\ 2,\ 3,\ 4),\ (1,\ 3)(2,\ 4),\ (1,\ 4,\ 3,\ 2)\}$ $G_2 =< \sigma_2 >= \{e,\ (1,\ 3,\ 2,\ 4),\ (1,\ 2)(3,\ 4),\ (1,\ 4,\ 2,\ 3)\}$ 4

5 G n G n

第十章　环

1 R 种 ($(+)$)

(i) R

(ii) ( ) $\forall a,\ b,\ c \in R, (ab)c = a(bc)$;

(iii) (配) $\forall a,\ b,\ c \in R, (a+b)c = ac+bc,\ a(b+c) = ab+ac$;

R .

(iv)( ) $\forall a, b \in R, ab = ba,$ R .

R $e = 1_R$ (v) $\forall a \in R,$ $a1_R = 1_R a = a,$

R .

1 R

(i) $a \in R, \quad 0a = a0 = 0;$

(ii) $a, b \in R, \quad (-a)b = a(-b) = -ab;$

(iii) $a, b \in R, \quad (-a)(-b) = ab;$

(iv) $n \in \mathbf{Z}, \quad a, b \in R, \quad (na)b = a(nb) = nab;$

(v) $a_i, b_j \in R,$

$$(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j.$$

(i) $0a = (0+0)a = 0a + 0a, \quad 0a = 0. \quad a0 = 0.$

(ii) $(-a)b + ab = ((-a)+a)b = 0a = 0,\ a(-b) + ab = a((-b)+b) = a0 = 0, \quad (-a)b = a(-b) = -ab.$

(iii), (iv) (v) (i) (ii)

2 R n $a, b, a_1, \ldots, a_r \in R$.

(i) $ab = ba, \qquad (a+b)^n = \sum_{k=0}^{n} \frac{n!}{k!(n-k)!} a^k b^{n-k}.$

(ii) $a_i a_j = a_j a_i,\ 1 \le i, j \le r,$

$$(a_1 + \cdots + a_r)^n = \sum_{i_1 + \cdots + i_r = n} \frac{n!}{i_1! \cdots i_r!} a_1^{i_1} \cdots a_r^{i_r}.$$

$\mathbf{1}$ $\mathbf{Z}$.

$\mathbf{Z}$ $a + b$ $0,\ a$

$-a.\ \mathbf{Z}$ $a \cdot b,$ $1.$

$\mathbf{Z}$

2 多项 $\mathbf{R}[X]$. $f(x) = a_n x^n + \cdots + a_1 x + a_0$,
$g(x) = b_n x^n + \cdots + b_1 x + b_0 \in \mathbf{R}[X]$. $\mathbf{R}[X]$

$$(f+g)(x) = (a_n + b_n)x^n + \cdots + (a_1 + b_1)x + (a_0 + b_0),$$

$\mathbf{R}[X]$

0, $f(x)$ $(-f)(x) = (-a_n)x^n + \cdots + (-a_1)x + (-a_0)$.

$f(x) = a_n x^n + \cdots + a_1 x + a_0, \quad a_n \neq 0, \quad g(x) = b_m x^m + \cdots + b_1 x + b_0, \quad b_m \neq 0,$

$\mathbf{R}[X]$ $(f \cdot g)(x) = c_{n+m} x^{n+m} + \cdots + c_1 x + c_0,$

$c_k = \Sigma_{i+j=k}\, a_i b_j, 0 \leq k \leq n+m,$

$$c_{n+m} = a_n b_m,\ c_{n+m-1} = a_n b_{m-1} + a_{n-1} b_m, \ldots,\ c_0 = a_0 b_0.$$

$\mathbf{R}[X]$ 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.

$\mathbf{R}[X]$

2 a R a **左零因** (
右零因), $b \in R$ ($c \in R$)
$ab = 0$ ($ca = 0$), a **零因** ,

4 $\mathbf{Z}/6\mathbf{Z} = \{\overline{0},\ \overline{1},\ \overline{2},\ \overline{3},\ \overline{4},\ \overline{5}\}$
$\overline{2} \cdot \overline{3} = 0$.

3 a 1_R R a **左**
(**右**), $b \in R$ ($c \in R$)
$ab = 1_R$ ($ca = 1_R$). b (c) a **右**
(**左**). a ,

4 R R **整**, R

5 R **域**, R R $R^* = R\backslash\{0\}$

6 R $a,\ b \in R,\ b \neq 0.$

$c \in R$ $a = bc,$ b **除** a a 被 b $b|a.$

把 b a , 把 a b **倍** .

$b,\ c$ b a .

R p 约 p

$b,\ c \in R$ $p = bc,$ b

c

$a,\ b \in R$ 伴 $u \in R$

$a = bu.$

7 $R,\ R'$ $f : R \longrightarrow R'$

, f

(i) $a,\ b \in I,$ $f(a+b) = f(a) + f(b);$

(ii) $a,\ b \in I,$ $f(ab) = f(a)f(b).$

f f ; f

f ; f f .

8 $R,\ R'$ R R'

R R'

9 R n

$a \in R$, $na = 0$, R **征** n.

R 征 0.

3 K 征 征比

K 征 n. n $1 <$

$n_1,\ n_2 < n$, $n = n_1 n_2$. $(n_1 1_{\mathbf{K}})(n_1 1_{\mathbf{K}}) = (n_1 n_2)1_{\mathbf{K}} = 0$.

K $(n_1 1_{\mathbf{K}}) = 0$ $(n_2 1_{\mathbf{K}}) = 0$. 征 n

4 R R

p, $a,\ b \in R$,

$$(a+b)^p = a^p + b^p.$$

2,

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \frac{p!}{k!(p-k)!} a^k b^{p-k} + b^p.$$

$1 \le k \le p-1$, $(p,\ k!(p-k)!) = 1$, $p \mid p\dfrac{(p-1)!}{k!(p-k)!}$.

R p, $\dfrac{p!}{k!(p-k)!} a^k b^{p-k} = 0.$

5 p $f(x) = a_n x^n + \cdots + a_1 x + a_0$

系

$$f(x)^p \equiv f(x^p) \pmod{p}.$$

$\mathbf{F}_p$ $\mathbf{F}_p[x]$ 4,

$f(x)^p = (a_n x^n)6p + \cdots + (a_1 x)^p + a_0^p = a_n (x^p)^n + \cdots + a_1 (x^p) + a_0 = f(x^p).$

$$f(x)^p \equiv f(x^p) \pmod{p}.$$

A　　$E = A \times A^*$.　　E　　R:

$(a,b)R(c,d)$　　$ad = bc$.　　R　　E

(i)　　$(a,b) \in E$,　　$(a,b)R(a,b)$.

(ii)　　$(a,b)R(c,d)$,　　$(c,d)R(a,b)$.

(iii) 传递　　$(a,b)R(c,d)$　　$(c,d)R(e,f)$,　　$(a,b)R(e,f)$.

$$\frac{a}{b} = C_{(a,b)} = \{(e,f)| \in E, (a,b)R(c,d)\} \qquad (a,b)$$

$$E/R$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}, \qquad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}.$$

E/R $\frac{0}{b}, \frac{a}{b}$ $\frac{-a}{b}.$

$(E/R)^* = E/R \setminus \{\frac{0}{b}\}$ $\frac{b}{b},$

$\frac{a}{b}$ $\frac{b}{a}.$

E/R A **分式** .

1 A R

1 $A = \mathbf{Z}$, $\mathbf{Z}$ $\mathbf{Z}$

, $\mathbf{Q}$.

2 $A = \mathbf{Z}/p\mathbf{Z}$, p A

$\mathbf{Z}/p\mathbf{Z}$ $p-$, $\mathbf{F}_p$ $GF(p)$..

3 K $A = \mathbf{K}[X]$

$\mathbf{K}[X]$ **项** , $\mathbf{K}(X)$.

$$\mathbf{K}(X) = \left\{ \frac{f(X)}{g(X)} \mid f(X),\ g(X) \in \mathbf{K}[X],\ g(X) \neq 0 \right\}.$$

1 R I R I R **想**,
$r \in R$ $a \in I$, $ra \in I$. I R
想, $r \in R$ $a \in I$, $ar \in I$. I
R **想**, R 想 想
1 $\{0\}$ R R 想 R **想**.

1 R I ( )

(i) $a, b \in I$, $a - b \in I$;

(ii) $r \in R$ $a \in I$, $ra \in I$. ($ar \in I$.)

(i) (ii) 道 I R

$\{A_i\}_{i \in I}$ R ( ) $\cap_{i \in I} A_i$ ( )

2 X R $\{A_i\}_{i\in I}$ R

X ( ) $\cap_{i\in I}A_i$ X ( ) .

(X).

X (X) . $X = \{a_1, \ldots, a_n\}$,

(X) $(a_1, \ldots, a_n)$, .

(a) 主 .

2 R $a \in R,\ X \subset R.$

(i) 主 (a)

$$(a) = \{ra + ar' + na + \sum_{i=1}^{m} r_i a s_i \mid r,\ s,\ r_i,\ s_i \in R,\ m \in \mathbf{N},\ n \in \mathbf{Z}\}.$$

(ii) R 1_R

$$(a) = \{ \sum_{i=1}^{m} r_i a s_i \mid r_i,\ s_i \in R,\ m \in \mathbf{N}, \}.$$

(iii) a R 心

$$(a) = \{ra + na \mid r \in R,\ n \in \mathbf{Z}\}.$$

(iv) $Ra = \{ra \mid r \in R\}$ ($aR = \{ar \mid r \in R\}$) R

( ) R $a \in Ra,\ a \in aR.$

R , R 主

2 Z 主

I $\mathbf{Z}$ $a \in I$ $0 = 0a \in I$
$-a = (-1)a \in I.$ I d I
$I = (d).$ $a \in I,$ q, r

$$a = dq + r, \quad 0 \leq r < d.$$

$a \in I$ $dq \in I,$ $r = a - dq \in I.$ $r < d$ d I
$r = 0,\ a = dq \in (d).$ $I \subset (d).$
$(d) \subset I.$ $I = (d).$ $\mathbf{Z}$

3 $\mathbf{Z}[X]$

4 $\mathbf{Z}[\sqrt{-5}]$

R I R I $(R,+)$

$$(a+I)+(b+I)=(a+b)+I,$$

R/I

$a+I=a'+I,\ b+I=b'+I$ $a=a'+r_1,\ b=b'+r_2,\quad r_1,\ r_2\in I.$ I $r_1b',\ a'r_2,\ r_1r_2\in I$.

$$ab+I=(a'+r_1)(b'+r_2)+I=a'b'+r_1b'+a'r_2+r_1r_2+I=a'b'+I.$$

R/I $(a+I)(b+I)=ab+I.$

4 R I R R/I

$$(a + I) + (b + I) = (a + b) + I,$$

$$(a + I)(b + I) = ab + I,$$

R R/I

R/I R I .

5 f R R' f $\ker(f)$ R

I R

$$s : R \longrightarrow R/I$$

$$r \longmapsto r + I$$

I

$s : R \longrightarrow R/I$ R R/I .

6 f R R' $R/\ker(f)$

$f(R)$ $\overline{f} : r + I \longmapsto f(r)$ $f = i \circ \overline{f} \circ s,$ s

R $R/\ker(f)$ $i : c \longmapsto c$ $f(R)$ R'

$$\begin{array}{ccc} R & \xrightarrow{f} & R' \\ \text{s} \downarrow & & \uparrow \text{i} \\ R/\ker(f) & \xrightarrow{\overline{f}} & f(R) \end{array}$$

3 P R P R , $P \neq R$,
$A, B,\ AB \subset P,$ $A \subset P$ $B \subset P.$

7 P R $P \neq R,$ $a, b \in R,$
$ab \in P$ $a \in P$ $b \in P,$ P P
R

5

6 p $P = (p) = p\mathbf{Z}$ $\mathbf{Z}$
$a,\ b,$ $ab \in P = (p),$ $p|ab.$ §1.4
2, $p|a$ $p\, b.$ $a \in P$ $b \in P.$ 7, $P = (p) = p\mathbf{Z}$
$\mathbf{Z}$

8 $1_R \neq 0$ R P

R/P

4 M R ( ) M R **最大 ( )**

, $M \neq R$, N, $M \subset N \subset R$, $N = M$

$N = R$.

9 R 大 ( ) 总

R ( ) $(\neq R)$ 大 ( )

10 R $R^2 = R$, (R

), R 大

11 R $1_R \neq 0$ M R

(i) M R R/M

(ii) R/M M 极

12 R $1_R \neq 0$

(i) R

(ii) R

(iii) 0 R

(iv) $R \to R'$

R $R[X]$.

$R[X]$

$$f(x)=a_nx^n+\cdots+a_1x+a_0,\quad g(x)=b_nx^n+\cdots+b_1x+b_0,$$

$f(x)$ $g(x)$

$$(f+g)(x)=(a_n+b_n)x^n+\cdots+(a_1+b_1)x+(a_0+b_0),$$

$R[X]$ 0,

$f(x)$

$$(-f)(x)=(-a_n)x^n+\cdots+(-a_1)x+(-a_0)$$

$R[X]$

$f(x) = a_n x^n + \cdots + a_1 x + a_0,\ a_n \neq 0, \quad g(x) = b_m x^m + \cdots + b_1 x + b_0,\ b_m \neq 0,$

$f(x) \qquad g(x)$

$$(f \cdot g)(x) = c_{n+m} x^{n+m} + \cdots + c_1 x + c_0,$$

$c_k = {}^{\Sigma}{}_{i+j=k}\, a_i b_j, 0 \leq k \leq n + m,$

$c_{n+m} = a_n b_m,\ c_{n+m-1} = a_n b_{m-1} + a_{n-1} b_m,\ \ldots,\ c_0 = a_0 b_0,$

$R[X]$ 1.

$R[X]$

1 $f(x) = x^6 + x^4 + x^2 + x + 1,\ g(x) = x^7 + x + 1 \in \mathbf{F}_2[x]$,

$$f(x) + g(x) = x^7 + x^6 + x^4 + x^2,$$

$f(x)g(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1.$

$$\begin{aligned}
&(x^6 + x^4 + x^2 + x + 1) \cdot (x^7 + x + 1) \\
=\ & x^{13} + x^{11} + x^9 + x^8 + x^7 + x^7 + x^5 + x^3 + x^2 + x \\
& + x^6 + x^4 + x^2 + x + 1 \\
=\ & x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1
\end{aligned}$$

$f(x) = a_n x^n + \cdots + a_1 x + a_0,\ a_n \neq 0,$ $f(x)$ **次** n, $\deg f = n$.

2 $\mathbf{Z}[X]$ $2x+3$ 1, x^2+2x+3 2, x^4+1 4, $x^8 + x^4 + x^3 + x + 1$ 8.

1 $f(x),\ g(x)$ R

$g(x) \neq 0.$ $q(x)$

$$f(x) = g(x)q(x) \qquad (1)$$

$g(x)$ $f(x)$ $f(x)$ $g(x)$ $g(x)|f(x).$

$g(x)$ $f(x)$, $f(x)$ $g(x)$.

$g(x)$ 能 $f(x)$ $f(x)$ 能 $g(x)$ $g(x) \nmid f(x).$

3 $\mathbf{Z}[X]$ $2x+3 \mid 2x^2+3x$, $x^2+1 \mid x^4-1$.

2 $f(x)$ R 了

1 $f(x)$ 外 $f(x)$ $f(x)$ **不 约**

, $f(x)$.

4 x^2+1 $\mathbf{Z}[x]$ $\mathbf{F}_2[x]$

5 $\mathbf{F}_2[x]$ $x,\ x+1.$

二 $x^2+x+1,$ $x^2,\ x^2+1=(x+1)^2,\ x^2+x=x(x+1).$

$x^3+x+1,\ x^3+x^2+1,$ $x^3,\ x^3+x,\ x^3+x^2,\ x^3+x^2+x,\ x^3+x^2+x+1=(x+1)(x^2+1),\ x^3+1=(x+1)(x^2+x+1).$

1 $f(x)=a_nx^n+\cdots+a_0,\ g(x)=x^m+\cdots+b_0$ R $q(x)$ $r(x)$ $f(x)=g(x)q(x)+r(x),\quad \deg r<\deg g.$

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

$$\begin{aligned}f(x)-a_nx^{n-m}\cdot g(x)=\ &(a_{n-1}-a_nb_{m-1})x^{n-1}+\cdots+(a_{n-m}-a_nb_0)x^{n-m}\\&+a_{n-m-1}x^{n-m-1}+\cdots+a_0.\end{aligned}$$

这说明 $f(x)-a_nx^{n-m}\cdot g(x)$ 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

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

因此, $q(x)=a_nx^{n-m}+g_1(x),\ r(x)=r_1(x)$ 为所求.

根据数学归纳法原理, 结论是成立的. 证毕.

1 **欧几里得 法.**

1 $f(x)$ R $a \in R,$

$q(x)$ $c = f(a)$ $f(x) = (x-a)q(x) + f(a).$

2 $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$ R

$a \in R,$ $x - a | f(x)$ $f(a) = 0.$

3 (2) $q(x)$ $f(x)$ $g(x)$ **完全** ,

$r(x)$ $f(x)$ $g(x)$ **余** .

6 $f(x)=x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1,\ g(x)=x^8+x^4+x^3+x+1\in\mathbf{F}_2[x]$, 求 $q_1(x)$ $r_1(x)$

$$f(x)=g(x)q_1(x)+r_1(x),\quad \deg r_1<\deg g_1.$$

解 逐 消 高

$$x^{13}+x^{11}+x^9+x^8+x^6+x^5+x^4+x^3+1-x^5(x^8+x^4+x^3+x+1)$$
$$=x^{11}+x^4+x^3+1,$$
$$x^{11}+x^4+x^3+1-x^3(x^8+x^4+x^3+x+1)$$
$$=x^7+x^6+1.$$

$$q_1(x)=x^5+x^3,\ r_1(x)=x^7+x^6+1.$$

公 公

$R[x]$ 公 公

$f(x),\ g(x) \in R[x]$. $d(x) \in R[x]$ $f(x),\ g(x)$ **公**

, (1) $d(x)|f(x),\ d(x)|g(x)$.

(2) $h(x)|f(x),\ h(x)|g(x),$ $h(x)|d(x)$.

$f(x),\ g(x)$ 公 $(f(x), g(x))$.

$f(x),\ g(x) \in R[x]$. $D(x) \in R[x]$ $f(x),\ g(x)$ **小公**

, (1) $f(x)|D(x),\ g(x)|D(x)$.

(2) $f(x)|h(x),\ g(x)|D(x),$ $D(x)|h(x)$.

$f(x),\ g(x)$ 公 $[f(x), g(x)]$.

广

$f(x),\ g(x)$ **K** $\deg g \geq 1.$ $r_0(x) = f(x),\ r_1(x) = g(x).$

$$
\begin{aligned}
r_0(x) &= r_1(x)q_1(x) + r_2(x), && 0 \leq \deg r_2 < \deg r_1,\\
r_1(x) &= r_2(x)q_2(x) + r_3(x), && 0 \leq \deg r_3 < \deg r_2,\\
&\cdots\cdots\\
r_{k-2}(x) &= r_{k-1}(x)q_{k-1}(x) + r_k(x), && 0 \leq \deg r_k < \deg r_{k-1},\\
r_{k-1}(x) &= r_k(x)q_k(x) + r_{k+1}(x), && \deg r_{k+1} = 0.
\end{aligned}
$$

骤 k $r_{k+1}(x) = 0,$

$$0 = \deg r_{k+1} < \deg r_k < \deg r_{k-1} < \ldots < \deg r_2 < \deg r_1 = \deg g,$$

$\deg g$

2 $f(x),\ g(x) \in \mathbf{K}[x]$, $\deg g \geq 1$, $(f(x), g(x)) = r_k(x)$, $r_k(x)$

$$r_{k-1}(x),\ r_{k-2}(x),\ \ldots, r_3(x),\ r_2(x),$$

$s(x),\ t(x) \in \mathbf{K}[x]$

$$s(x)f(x) + t(x)g(x) = (f(x), g(x)).$$

3 $f(x),\ g(x) \in \mathbf{K}[x]$, $s(x),\ t(x) \in \mathbf{K}[x]$

$$s(x)f(x) + t(x)g(x) = (f(x), g(x)).$$

$f(x)$ $g(x)$ ( )

$(f(x), g(x)) = 1$.

7 $f(x) = x^{13} + x^{11} + x^9 + x^8 + x^6 + x^5 + x^4 + x^3 + 1,\ g(x) = x^8 + x^4 + x^3 + x + 1 \in \mathbf{F}_2[x]$, $s(x),\ t(x)$

$$s(x)f(x) + t(x)g(x) = (f(x), g(x)).$$

$$\begin{array}{lll}
f(x) = g(x)q_1(x) + r_1(x), & q_1(x) = x^5 + x^3, & r_1(x) = x^7 + x^6 + 1, \\
g(x) = r_1(x)q_2(x) + r_2(x), & q_2(x) = x + 1, & r_2(x) = x^6 + x^4 + x^3, \\
r_1(x) = r_2(x)q_3(x) + r_3(x), & q_3(x) = x + 1, & r_3(x) = x^5 + x^3 + 1, \\
r_2(x) = r_3(x)q_4(x) + r_4(x), & q_4(x) = x, & r_4(x) = x^3 + x, \\
r_3(x) = r_4(x)q_5(x) + r_5(x), & q_5(x) = x^2, & r_5(x) = 1.
\end{array}$$

$$
\begin{aligned}
r_5(x) &= r_3(x) + q_5(x)(r_2(x) + r_3(x)q_4(x)) \\
&= -q_5(x)r_2(x) + (x^3+1)(r_1(x) + r_2(x)q_3(x)) \\
&= (x^3+1)r_1(x) + (x^4+x^3+x^2+x+1)(g(x) + r_1(x)q_2(x)) \\
&= (x^4+x^3+x^2+x+1)g(x) + (x^5+x^3)(f(x) + g(x)q_1(x)) \\
&= (x^5+x^3)f(x) + (x^{10}+x^6+x^4+x^3+x^2+x+1)g(x).
\end{aligned}
$$

$$
s(x) = x^5 + x^3,\ t(x) = x^{10} + x^6 + x^4 + x^3 + x^2 + x + 1.
$$

4 $R[X]$ $m(x)$. $f(x),\ g(x)$
$m(x)$, $m(x) \mid f(x)-g(x)$. $f(x) \equiv g(x) \pmod{m(x)}$.
$m(x)$. $f(x) \not\equiv g(x) \pmod{m(x)}$.
1, $f(x)$ $m(x)$ $r(x)$
$m(x)$ $r(x)$ $f(x)$ $m(x)$,
$(f(x) \pmod{m(x)})$.
$p(x)$ $R[X]$ $(p(x)) = \{f(x) \mid p(x)|f(x)\}$
$R[X]$ $R/(p(x))$.

$$f(x) + g(x) = ((f+g)(x) \pmod{p(x)}),$$

$$f(x)g(x) = ((fg)(x) \pmod{p(x)}).$$

4 **K** $p(x)$ $\mathbf{K}[X]$

$\mathbf{K}[X]/(p(x))$

只需 $\mathbf{K}[X]/(p(x))$ $f(x) \pmod{p(x)}$

$f(x) \not\equiv 0 \pmod{p(x)}$ $f(x)$,

$(f(x), p(x)) = 1.$ 3 , $s(x),\ t(x)$

$$s(x)f(x) + t(x)p(x) = 1.$$

$$s(x)f(x) \equiv 1 \pmod{p(x)}.$$

$f(x) \pmod{p(x)}$ $s(x) \pmod{p(x)}$

11 $\mathbf{K} = \mathbf{Z}/p\mathbf{Z}$ p $p(x)$ $\mathbf{K}[X]$ n

$$\mathbf{K}[X]/(p(x)) = \{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \mid a_i \in \mathbf{K}\}.$$

$\mathbf{F}_{p^n}$. p^n.

$\mathbf{F}_{p^n}$

$$f(x) + g(x) = ((f+g)(x) \pmod{p(x)}),$$

$$f(x)g(x) = ((fg)(x) \pmod{p(x)}).$$

12 $\mathbf{F}_2 = \mathbf{Z}/2\mathbf{Z}$. $p(x) = x^8 + x^4 + x^3 + x + 1$ $\mathbf{F}_2[X]$

8

$$\mathbf{F}_{2^8} = \mathbf{F}_2[X]/(x^8+x^4+x^3+x+1) = \{a_7x^7 + \cdots + a_1x + a_0 \mid a_i \in \{0,1\}\}.$$

$\mathbf{F}_{2^8}$

$$f(x) + g(x) = ((f+g)(x) \pmod{x^8 + x^4 + x^3 + x + 1}),$$

$$f(x)g(x) = ((fg)(x) \pmod{x^8 + x^4 + x^3 + x + 1}).$$

第十一章　域和 Galois 理论

1 **F** **K** **F** **F** **K**

扩 .

F **K** 扩 $1_{\mathbf{F}} = 1_{\mathbf{K}}$. **F** **K**

间 $[\mathbf{F} : \mathbf{K}]$ **F** **K** 间 维

F **K** **扩张** **扩张**, $[\mathbf{F} : \mathbf{K}]$

1 **E** **F** **F** **K**

$$[\mathbf{E} : \mathbf{K}] = [\mathbf{E} : \mathbf{F}][\mathbf{F} : \mathbf{K}].$$

$\{\alpha_i\}_{i \in I}$ **F** **K** $\{\beta_j\}_{j \in J}$ **E** **F**

$\{\alpha_i \beta_j\}_{i \in I, j \in J}$ **E** **K**

$\{\alpha_i \beta_j\}_{i \in I, j \in J}$ **E** **K**

$c \in \mathbf{E}$, $\{\beta_j\}_{j \in J}$ **E** **F** $b_j \in \mathbf{F},\ j \in J$

$$c = \sum_{j \in J} b_j \beta_j.$$

$\{\alpha_i\}_{i \in I}$ **F** **K** $a_{ij} \in \mathbf{K},\ i \in I$

$$b_j = \sum_{i \in I} a_{ij} \alpha_i.$$

$$c = \sum_{i \in I, j \in J} a_{ij} \alpha_i \beta_j.$$

$\{\alpha_i \beta_j\}_{i \in I, j \in J}$ **K**

$a_{ij} \in \mathbf{K},\ i \in I$

$$\sum_{i \in I, j \in J} a_{ij} \alpha_i \beta_j = 0 \qquad \sum_{j \in J} \left(\sum_{i \in I} a_{ij} \alpha_i \right) \beta_j = 0.$$

$\{\beta_j\}_{j \in J}$ **E** **F**

$$\sum_{i \in I} a_{ij} \alpha_i = 0, \quad j \in J.$$

$\{\alpha_i\}_{i \in I}$ **F** **K**

$$a_{ij} = 0 \quad i \in I,\ j \in J.$$

$$[\mathbf{E} : \mathbf{K}] = [\mathbf{E} : \mathbf{F}][\mathbf{F} : \mathbf{K}].$$

$\mathbf{E}$ $\mathbf{K}$ $\mathbf{E}$ $\mathbf{F}$

$\mathbf{F}$ $\mathbf{K}$

1 **R** **Q** **C** **R**

2 $\mathbf{Q}(\sqrt{2})$ **Q** 张 $[\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2$.

F $X \subset \mathbf{F}$, X (

) X X (

). **F** **K** $X \subset \mathbf{F}$, $\mathbf{K} \cup X$ (

) X **在 K 上** (

), $\mathbf{K}(X)$ ($\mathbf{K}[X]$). 注 $\mathbf{K}[X]$

$X = \{u_1, \ldots, u_n\}$, **F** $\mathbf{K}(X)$ ($\mathbf{K}[X]$)

$\mathbf{K}(u_1, \ldots, u_n)$ ($\mathbf{K}[u_1, \ldots, u_n]$). $\mathbf{K}(u_1, \ldots, u_n)$

K 张 $X = \{u\}$, $\mathbf{K}(u)$ **K** 张

2 $\mathbf{F}$ $\mathbf{K}$ $u,\ u_1,\ \ldots,\ u_n \in \mathbf{F},$ $X \subset \mathbf{F},$

(i) $\mathbf{K}[u]$ 形 $f(u)$ f $\mathbf{K}$ ($f \in \mathbf{K}[x]$).

(ii) $\mathbf{K}[u_1, \ldots, u_n]$ 形 $f(u_1, \ldots, u_n)$ f $\mathbf{K}$ n ($f \in \mathbf{K}[x_1, \ldots, x_n]$).

(iii) $\mathbf{K}[X]$ 形 $f(u_1, \ldots, u_n)$ $n \in \mathbf{N},\ u_1,\ \ldots,\ u_n \in X,\ f$ $\mathbf{K}$ n ($f \in \mathbf{K}[x_1, \ldots, x_n]$).

(iv) $\mathbf{K}(u)$ 形 $\dfrac{f(u)}{g(u)}$ $f(u)/g(u)$ $f,\ g \in \mathbf{K}[x],\ g(u) \neq 0.$

(v) $\mathbf{K}(u_1, \ldots, u_n)$ $\dfrac{f(u_1, \ldots, u_n)}{g(u_1, \ldots, u_n)}$

$f,\ g \in \mathbf{K}[x_1, \ldots, x_n],\ g(u_1, \ldots, u_n) \neq 0.$

(vi) $\mathbf{K}(u_1, \ldots, u_n)$ $\dfrac{f(u_1, \ldots, u_n)}{g(u_1, \ldots, u_n)}$

$n \in \mathbf{N},\ f,\ g \in \mathbf{K}[x_1, \ldots, x_n],\ u_1, \ldots, u_n \in X,\ g(u_1, \ldots, u_n) \neq 0.$

(vii) $v \in \mathbf{K}(X)$ ($\mathbf{K}[X]$),

$X' \subset X,$ $v \in \mathbf{K}(X')$ ($\mathbf{K}[X']$).

2 $\mathbf{F}$ $\mathbf{K}$ $\mathbf{F}$ u $\mathbf{K}$ **代**

, $f \in \mathbf{K}[x]$ $f(u) = 0$. $\mathbf{F}$

u $\mathbf{K}$ **超越** , 何 $f \in \mathbf{K}[x]$

$f(u) = 0$. $\mathbf{F}$ $\mathbf{K}$ **代** , $\mathbf{F}$ $\mathbf{K}$

$\mathbf{F}$ $\mathbf{K}$ **超越** , $\mathbf{F}$ 至少

$\mathbf{K}$ 超越

$u \in \mathbf{K}$, u $x - u \in \mathbf{K}[x]$ u $\mathbf{K}$

3 **F** **K** $u \in \mathbf{F}$ **K**

K $\mathbf{K}(u) \cong \mathbf{K}(x)$.

u **K** $g(x)$,

$g(u) \neq 0$. $\mathbf{K}(x)$ $\mathbf{K}(u)$

$$\sigma : \frac{F(x)}{g(x)} \longmapsto \frac{F(u)}{g(u)}.$$

σ σ σ

$\mathbf{F}$ $\mathbf{K}$ $u \in \mathbf{F}$ $\mathbf{K}$

$\mathbf{K}$ $f(x)$ $f(u) = 0$.

$u \in \mathbf{F}$ $\mathbf{K}$ $\mathbf{K}$

$f(x)$ $f(u) = 0$.

$f(x)$. $f(x)$ $f(x)$

3 $\mathbf{F}$ $\mathbf{K}$ $u \in \mathbf{F}$ $\mathbf{K}$ 引

u (**极**

). u $\mathbf{K}$ $\deg f$. u

u **共轭根**.

4 $\mathbf{F}$ $\mathbf{K}$ $u \in \mathbf{F}$ $\mathbf{K}$

(i) $\mathbf{K}(u) = \mathbf{K}[u]$.

(ii) $\mathbf{K}(u) \cong \mathbf{K}[x]/(f)$, $f \in \mathbf{K}[x]$ $f(u) = 0$

n

(iii) $[\mathbf{K}(u) : \mathbf{K}] = n$.

(iv) $\{1, u, u^2, \ldots, u^{n-1}\}$ $\mathbf{K}$ 向量 $\mathbf{K}(u)$

(v) $\mathbf{K}(u)$ $a_0+a_1u+\cdots+a_{n-1}u^{n-1}$, $a_i \in$ $\mathbf{K}$.

3 $x^2 - x - 1$ $\mathbf{Q}$

4 $x^3 - 3x - 1$ $\mathbf{Q}$

5 $\sigma : \mathbf{K} \to \mathbf{L}$ u $\mathbf{K}$ 某

v $\mathbf{L}$ 某

(i) u $\mathbf{K}$ v $\mathbf{L}$

(ii) u $f \in \mathbf{K}[x]$ v

$\sigma f \in \mathbf{L}[x]$

σ $\mathbf{K}(u) \cong \mathbf{L}(v)$, u v.

6 $\mathbf{E}$ $\mathbf{F}$ $\mathbf{K}$ $u \in \mathbf{E}$ $v \in \mathbf{F}$. u v $f \in \mathbf{K}[x]$ $\mathbf{K}$ $\mathbf{K}(u) \cong \mathbf{L}(v)$, u v.

7 $\mathbf{K}$ $f \in \mathbf{K}[x]$ n

$\mathbf{K}$ $\mathbf{F} = \mathbf{K}(u)$

(i) $u \in \mathbf{F}$ f

(ii) $[\mathbf{K}(u) : \mathbf{K}] \leq n,$ f $\mathbf{K}[x]$

$\mathbf{K}$ $f \in \mathbf{K}[x]$ n

α $f(x)$ α $\mathbf{K}$ $\mathbf{F} = \mathbf{K}(\alpha),$

$[\mathbf{K}(\alpha) : \mathbf{K}] = n.$

1 $\mathbf{E}$ $\mathbf{F}$ $\mathbf{K}$ $\sigma : \mathbf{E} \to \mathbf{F}$ $\mathbf{K}$- , σ $\mathbf{K}$ $\sigma : \mathbf{F} \to \mathbf{F}$ $\mathbf{K}$- , σ $\mathbf{K}$- $\mathbf{F}$ $\mathbf{K}$- $\mathbf{F}$ $\mathbf{K}$ **伽略华 (Galois)** , $Aut_{\mathbf{K}}\mathbf{F}$.

1 $\mathbf{F}$ $\mathbf{K}$ $f \in \mathbf{K}[x]$. $u \in \mathbf{F}$ f $\sigma \in Aut_{\mathbf{K}}\mathbf{F}$, $\sigma(u)$ f

$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbf{K}[x]$. $u \in \mathbf{F}$ $\sigma \in Aut_{\mathbf{K}}\mathbf{F}$,

$$\sigma f(u) = \sigma(a_n)\sigma(u)^n + \cdots + \sigma(a_1)\sigma(u) + \sigma(a_0) = a_n\sigma(u)^n + \cdots + a_1\sigma(u) + a_0 = f(\sigma(u)).$$

2 **F** **K** **E** H $Aut_{\mathbf{K}}\mathbf{F}$

(i) $\mathbf{E}' = \{v \in \mathbf{F} \mid \sigma(v) = v,\ \sigma \in H\}$ **F**

(ii) $H' = \{\sigma \in Aut_{\mathbf{K}}\mathbf{F} \mid \sigma(u) = u,\ u \in \mathbf{E}\} = Aut_{\mathbf{E}}\mathbf{F}$ $Aut_{\mathbf{K}}\mathbf{F}$

$\mathbf{E}'$ H **F**

2 **F** **K** **F** **K-** **Galois** ,

Galois $Aut_{\mathbf{K}}\mathbf{F}$ **K**.

3 (Galois 本) $\mathbf{F}$ $\mathbf{K}$ Galois

Galois $Aut_{\mathbf{K}}\mathbf{F}$

$$\mathbf{E} \mapsto H' = Aut_{\mathbf{E}}\mathbf{F}$$

(i)

$Aut_{\mathbf{K}}\mathbf{F}$ $[\mathbf{F} : \mathbf{K}]$.

(ii) $\mathbf{F}$ $\mathbf{E}$ Galois $\mathbf{E}$ $\mathbf{K}$ Galois

$H' = Aut_{\mathbf{E}}\mathbf{F}$ $G = Aut_{\mathbf{K}}\mathbf{F}$

G/H' ( ) $\mathbf{E}$ $\mathbf{K}$ Galois $Aut_{\mathbf{K}}\mathbf{E}$.

1 **K** $f \in \mathbf{K}[x]$ ≥ 1 **K**

F f **K** **裂**, f $\mathbf{F}[x]$

$\mathbf{F} = \mathbf{K}(u_1, \ldots, u_n)$, $u_1, \ldots, u_n$ f **F**

S $\mathbf{K}[x]$ ≥ 1 **K**

F S **K** **裂**, S

f $\mathbf{F}[x]$ **F** S **K**

1 $\mathbf{K}$ $f \in \mathbf{K}[x]$ $n \geq 1$. f 裂 $\mathbf{F}$ $[\mathbf{F} : \mathbf{K}] \leq n!$.

2 $\mathbf{F}$

(i) $f \in \mathbf{F}[x]$ $\mathbf{F}$

(ii) $f \in \mathbf{F}[x]$ $\mathbf{F}$

(iii) $f \in \mathbf{F}[x]$

(iv) $\mathbf{F}$ ($\mathbf{F}$ 已).

2 $\mathbf{F}$ $\mathbf{F}$ 闭 $\mathbf{F}$

2

第十二章　域的结构

1 $\mathbf{F}$ $\mathbf{K}$ $a_1, a_2, \ldots, a_n$ $\mathbf{F}$ n

$a_1, a_2, \ldots, a_n$ $\mathbf{K}$ **相** ,

$f \in \mathbf{K}[x_1, \ldots, x_n]$ S n $a_1, a_2, \ldots, a_n,$

$$f(a_1, a_2, \ldots, a_n) = 0.$$

$a_1, a_2, \ldots, a_n$, $a_1, a_2, \ldots, a_n$

注 谓 $a_1, a_2, \ldots, a_n$ $f \in \mathbf{K}[x_1, \ldots, x_n]$

$f(a_1, a_2, \ldots, a_n) = 0,$

$f = 0.$

1 圆周率 $\pi = 3.14\cdots$ $\mathbf{Q}$ $e = 2.718\cdots$ $\mathbf{Q}$

1 **F** **K** **F** **K**

$\theta_1, \ldots, \theta_t$ **F** $\mathbf{K}(\theta_1, \ldots, \theta_t)$

$\mathbf{F}_q$　q　p　$\mathbf{F}_q$　$\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$, $\mathbf{F}_p$　$n = [\mathbf{F}_q : \mathbf{F}_p]$, $q = p^n$, q　p

$\mathbf{F}_q^* = \mathbf{F}_q \setminus \{0\}$　$q-1$

讨　$\mathbf{F}_q^*$　质

1　$\mathbf{F}_q^*$　a　$q-1$.

1　$\mathbf{F}_q$　g　,　$\mathbf{F}_q^*$　$q-1$

g　$\mathbf{F}_q$　$\mathbf{F}_q = \{0,\ g^0 = 1,\ g,\ \ldots,\ g^{q-2}\}$..

2 g $\mathbf{F}_q$ g^d $\mathbf{F}_q$ d $q-1$ $(d, q-1) = 1$.

$\mathbf{F}_q$ $\varphi(q-1)$

1 $q = p^n$, p $d|q-1$, $\mathbf{F}_q$ d

2 p g 遍历 p 化 p 原

3 $\mathbf{F}_q$ $q = p^n$ $x^q - x = 0$. 确切 $\mathbf{F}_q$ $q = p^n$, $x^q - x$ $\mathbf{F}_p$ q

4 $\mathbf{F}_q$ $q = p^n$ σ $\mathbf{F}_q$

$\sigma : a \longmapsto a^p$. σ $\mathbf{F}_q$ $\mathbf{F}_q$ σ 动

$\mathbf{F}_p$ σ n

4 σ **Frobenius** .

5 $\mathbf{F}_q$ $q = p^n$ σ $\mathbf{F}_q$

$\sigma : a \longmapsto a^p$. α $\mathbf{F}_q$ α $\mathbf{F}_p$ 轭

$\sigma^j(\alpha) = \alpha^{p^j}$.

具体　造.　　§10.4　　4,　　造

$\mathbf{F}_p$　　d

$p(x)$　　$\mathbf{F}_p[X]$　　d　　$\mathbf{F}_p[x]/(p(x))$

$$f(x) + g(x) = ((f + g)(x) \pmod{p(x)}),$$

$$f(x)g(x) = ((fg)(x) \pmod{p(x)}).$$

$\mathbf{F}_p[x]/(p(x))$　　§11.1　　2,

$\mathbf{F}_p$　　d　　$\mathbf{F}_q$　　$GF(q)$,

$q = p^d$.

$\mathbf{F}_2/(x^4 + x + 1)$　　x,

1 x^4+x+1 $\mathbf{F}_2[x]$ $\mathbf{F}_2[x]/(x^4+x+1)$ $\mathbf{F}_{2^4}$

$\mathbf{F}_2[x]$ ≤ 2 $x,\ x+1,\ x^2+x+1,$

$$x^4+x+1 = x(x^3+1)+1,\ x^4+x+1 = (x+1)(x^3+x^2+x)+1,$$

$$x^4+x+1 = (x^2+x+1)(x^2+x)+1,$$

$$x \not| x^4+x+1,\ x+1 \not| x^4+x+1,\ x^2+x+1 \not| x^4+x+1\ .$$

x^4+x+1 $\mathbf{F}_2[x]$ $\mathbf{F}_2[x]/(x^4+x+1)$ $\mathbf{F}_{2^4}$

2 $\mathbf{F}_{2^4} = \mathbf{F}_2[x]/(x^4 + x + 1)$ $g(x)$, $g(x)^t$, $t = 0, 1, \ldots, 14$

$$|\mathbf{F}_{2^4}^*| = 15 = 3 \cdot 5,$$

$$g(x)^3 \not\equiv 1 \pmod{x^4 + x + 1}, \quad g(x)^5 \not\equiv 1 \pmod{x^4 + x + 1}$$

$g(x)$

$$g(x) = x,$$

$$x^3 \equiv x^3 \not\equiv 1 \pmod{x^4 + x + 1}, \quad x^5 \equiv x^2 + x \not\equiv 1 \pmod{x^4 + x + 1},$$

$g(x) = x$ $\mathbf{F}_2[x]/(x^4 + x + 1)$

$$t = 0, 1, 2, \ldots, 14, \qquad g(x)^t \pmod{x^4 + x + 1}:$$

$$g(x)^0 \equiv 1, \quad g(x)^1 \equiv x, \quad g(x)^2 \equiv x^2,$$
$$g(x)^3 \equiv x^3, \quad g(x)^4 \equiv x + 1, \quad g(x)^5 \equiv x^2 + x,$$
$$g(x)^6 \equiv x^3 + x^2, \quad g(x)^7 \equiv x^3 + x + 1, \quad g(x)^8 \equiv x^2 + 1,$$
$$g(x)^9 \equiv x^3 + x, \quad g(x)^{10} \equiv x^2 + x + 1, \quad g(x)^{11} \equiv x^3 + x^2 + x,$$
$$g(x)^{12} \equiv x^3 + x^2 + x + 1, \quad g(x)^{13} \equiv x^3 + x^2 + 1, \quad g(x)^{14} \equiv x^3 + 1.$$

$$g(x)^t, \ (t, \varphi(15)) = 1:$$

$$g(x)^1 = x, \quad g(x)^2 = x^2, \quad g(x)^4 = x + 1,$$
$$g(x)^7 = x^3 + x + 1, \quad g(x)^8 = x^2 + 1, \quad g(x)^{11} = x^3 + x^2 + x,$$
$$g(x)^{13} = x^3 + x^2 + 1, \quad g(x)^{14} = x^3 + 1.$$

3 $\mathbf{F}_{2^8} = \mathbf{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$ $g(x)$.

$|\mathbf{F}_{2^8}^*| = 255 = 3 \cdot 5 \cdot 17,$

$$g(x)^{15} \not\equiv 1,\ g(x)^{51} \not\equiv 1,\ g(x)^{85} \not\equiv 1 \pmod{x^8 + x^4 + x^3 + x + 1}$$

$g(x)$

$g_1(x) = x,$

$$g_1(x)^{15} \equiv x^5 + x^3 + x^2 + x + 1, \qquad g_1(x)^{51} \equiv 1,$$
$$g_1(x)^{85} \equiv x^7 + x^5 + x^4 + x^3 + x^2 + 1 \pmod{x^8 + x^4 + x^3 + x + 1}.$$

$g_1(x) = x$ $\mathbf{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$

$$g_2(x) = x + 1,$$

$$g_2(x)^2 \equiv x^2 + 1, \qquad g_2(x)^3 \equiv x^3 + x^2 + x + 1,$$

$$g_2(x)^4 \equiv x^4 + 1, \qquad g_2(x)^7 \equiv x^7 + x^6 + x^5 + x^4 + x^3 + x^2 +$$

$$g_2(x)^8 \equiv x^4 + x^3 + x, \qquad g_2(x)^{15} \equiv x^5 + x^4 + x^2 + 1,$$

$$g_2(x)^{16} \equiv x^6 + x^4 + x^3 + x^2 + x + 1, \quad g_2(x)^{32} \equiv x^7 + x^6 + x^5 + x^2 + 1,$$

$$g_2(x)^{48} \equiv x^6 + x^4 + x + 1, \qquad g_2(x)^{51} \equiv x^3 + x^2,$$

$$g_2(x)^{83} \equiv x^7 + x^6 + x^4, \qquad g_2(x)^{85} \equiv x^7 + x^5 + x^4 + x^3 + x^2 + 1.$$

$$g_2(x)^{15} \not\equiv 1, \quad g_2(x)^{51} \not\equiv 1, \quad g_2(x)^{85} \not\equiv 1 \pmod{x^8 + x^4 + x^3 + x + 1}.$$

$g_2(x) = x + 1$ $\qquad$ $\mathbf{F}_2[x]/(x^8 + x^4 + x^3 + x + 1)$

6 $\mathbf{F}_{p^n}$ $\mathbf{F}_{p^d},\ (d|n),$ $\mathbf{F}_{p^n}$ $\mathbf{F}_p$

7 $q = p^n,$ $x^q - x$ $\mathbf{F}_p[x]$

$d|n.$

n $\mathbf{F}_{p^n}[x]$ $\dfrac{p^n - p}{n}$ n

8 $p,\ r$ $\mathbf{F}_p$ $\dfrac{x^r - 1}{x - 1}$

$\mathrm{ord}_r(p)$

第十三章　椭圆曲线

K **K** Weierstrass

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad (1)$$

$a_1,\ a_2,\ a_3,\ a_4,\ a_6 \in \mathbf{K}$.

K 2

$$(y + \frac{1}{2}a_1x + \frac{1}{2}a_3)^2 = x^3 + (\frac{1}{4}a_1^2 + a_2)x^2 + (\frac{1}{2}a_1a_3 + a_4)x + \frac{1}{4}a_3^2 + a_6$$

$$(2y + a_1x + a_3)^2 = 4x^3 + b_2x^2 + 2b_4x + b_6,$$

$$\begin{cases} b_2 = a_1^2 + 4a_2, \\ b_4 = a_1a_3 + 2a_4, \quad (2) \\ b_6 = a_3^2 + 4a_6. \end{cases}$$

K 2, 3 继续

$$(2y+a_1x+a_3)^2 = 4(x+\frac{1}{12}b_2)^3+(-\frac{1}{12}b_2^2+2b_4)(x+\frac{1}{12}b_2)+(\frac{1}{216}b_2^3-\frac{1}{6}b_2b_4+b_6),$$

$$108^2(2y+a_1x+a_3)^2 = 36^3(x+\tfrac{1}{12}b_2)^3 - 27c_4\cdot 36(x+\tfrac{1}{12}b_2) - 54c_6,$$

$$\begin{cases} c_4 = b_2^2 - 24b_4, \\ c_6 = -b_2^3 + 36b_2b_4 - 216b_6. \end{cases} \quad (3)$$

$$\begin{cases} X = 36(x+\frac{1}{12}b_2) \\ \\ Y = 108(2y+a_1x+a_3) \end{cases} \qquad \begin{cases} x = \frac{1}{36}X - \frac{1}{12}b_2 \\ \\ y = \frac{1}{216}Y - \frac{1}{2}a_1(\frac{1}{36}X - \frac{1}{12}b_2) - \frac{1}{2}a_3, \end{cases}$$

$$Y^2 = X^3 - 27c_4X - 54c_6. \quad (4)$$

判 $1728\Delta = c_4^3 - c_6^2.$

$\mathbf{K}$, Weierstrass (1)

$$\Delta = -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6, \quad (5)$$

$$b_8 = a_1^2 a_6 - a_1 a_3 a_4 + 4a_2 a_6 + a_2 a_3^2 - a_4^2 \ (\ i.e.\ 4b_8 = b_2 b_6 - b_4^2). \quad (6)$$

1 $\Delta \neq 0$, **K** 点

$$E := \{(x, y) \mid y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6\}\cup\{O\},$$

$a_1,\ a_2,\ a_3,\ a_4,\ a_6 \in \mathbf{K}, \{O\}$ 穷远点 **K** **椭圆曲** . $j = c_4^3/\Delta$ 椭 曲 E j**- 变量**, $j(E)$.

Weierstrass 齐

$$Y^2Z + a_1XYZ + a_3Y = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \quad (8)$$

$a_1,\ a_2,\ a_3,\ a_4,\ a_6 \in \mathbf{K}$. 1 穷远点 O 齐 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) $\mathbf{K}$ 2, 3 Weierstrass

$$y^2 = x^3 + a_4x + a_6, \quad \Delta = -16(4a_4^3 + 27a_6^2), \quad j = 1728\frac{4a_4^3}{4a_4^3 + 27a_6^2}.$$

(ii) $\mathbf{K}$ 2 , $j(E) \neq 0$ Weierstrass

$$y^2 + xy = x^3 + a_2x^2 + a_6, \quad \Delta = a_6, \quad j = 1/a_6.$$

(iii) $\mathbf{K}$ 2 , $j(E) = 0$ Weierstrass

$$y^2 + a_3y = x^3 + a_4x + a_6, \quad \Delta = a_3^4, \quad j = 0.$$

(iv) $\mathbf{K}$ 3 , $j(E) \neq 0$ Weierstrass

$$y^2 = x^3 + a_2x^2 + a_6, \quad \Delta = -a_2^3a_6, \quad j = -a_2^3/a_6.$$

(v) $\mathbf{K}$ 3 , $j(E) = 0$ Weierstrass

$$y^2 = x^3 + a_4 x + a_6, \quad \Delta = -a_4^3, \quad j = 0.$$

E Weierstrass (7) **K**

E $\oplus$.

则 P, Q E L P Q

(P $P = Q$), R L E

L' R O $P \oplus Q$ L' E

1 E $\oplus$

(i) L E P, Q, R ( ),

$$(P \oplus Q) \oplus R = O.$$

(ii) $P \in E$, $P \oplus O = P$.

(iii) $P, Q \in E$, $P \oplus Q = Q \oplus P$.

(iv) $P \in E$, $-P$, $P \oplus (-P) = O$.

(v) $P, Q, R \in E$, $(P \oplus Q) \oplus R = P \oplus (Q \oplus R)$.

E $\oplus$

E K

$$E(\mathbf{K}) := \{(x, y)\mathbf{K} \times \mathbf{K} \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{O\}, \quad (9)$$

E

1 精

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

$$-P_1 = (x_1, -y_1 - a_1x_1 - a_3).$$

取 $\begin{cases} \lambda = \dfrac{y_2 - y_1}{x_2 - x_1} & \text{如果 } x_1 \neq x_2, \\ \lambda = \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3} & \text{如果 } x_1 = x_2. \end{cases}$

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 $\lambda=\dfrac{y_2-y_1}{x_2-x_1}$.

$x_1 = x_2$ L P 切 其 λ

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}.$$

$y = \lambda x + \mu$ 带 $F(x, y) = 0$

$$F(x, \lambda x + \mu) = -x^3 + (\lambda^2 + a_1\lambda - a_2)x^2 + (2\lambda\mu + a_1\mu - a_4)x + \mu^2 - a_6 = 0.$$

因 $P_1,\ P_2$ P_3 E 上三 所以上述 x 三 解 $x_1,\ x_2,\ x_3$. $F(x, \lambda x + \mu) = c(x - x_1)(x - x_2)(x - x_3)$.

因此 $c = -1$ 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　域 $\mathbf{R}$　　运　法　　几何意

$\mathrm{chap}(\mathbf{R}) \neq 2,\ 3,$　　$\mathbf{R}$　　E　　Weierstrass　　可

$E:\ y^2 = x^3 + a_4 x + a_6,$

判别式 $\Delta = -16(4a_4^3 + 27a_6^2) \neq 0$. E 在 $\mathbf{R}$　　运　规　　:

$P_1 = (x_1, y_1),\ P_2 = (x_2, y_2)$　　E　　O　　无

穷远

(1) $O + P_1 = P_1 + O$;　　(2) $-P_1 = (x_1, -y_1)$;

(3)　　$P_3 = (x_3, y_3) = P_1 + P_2 \neq O,$

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2, \\ y_3 = \lambda(x_1 - x_3) - y_1. \end{cases}$$

其中

$$\begin{cases} \lambda = \dfrac{y_2 - y_1}{x_2 - x_1} & \text{如果 } x_1 \neq x_2, \\ \lambda = \dfrac{3x_1^2 + a_4}{2y_1} & \text{如果 } x_1 = x_2. \end{cases}$$

$P_1 = (x_1, y_1),\ P_2 = (x_2, y_2)$ E O

$-P_1$ P_1 O L 与 E 交 换句话说 $-P_1$ P_1 x 轴 对称

P_1 与 P_2 $P_1 + P_2 = P_3 = (x_3, y_3)$ P_1 P_2 L 与 E 交 R x 轴 对称 $P_3 = -R.$

素　$\mathbf{F}_p\ (p>3)$　　E.

素　$\mathbf{F}_p$　特征不　$2,\ 3,$　　素　$\mathbf{F}_p$　　E

Weierstrass　　$E:\ y^2=x^3+a_4x+a_6,$

$\Delta=-16(4a_4^3+27a_6^2)\neq 0\ .\ E$　　$\mathbf{R}$

$P_1=(x_1,y_1),\ P_2=(x_2,y_2)$　　E　　O

(1) $O+P_1=P_1+O;$　　(2) $-P_1=(x_1,-y_1);$

(3)　　$P_3=(x_3,y_3)=P_1+P_2\neq O,$

$$\begin{cases} x_3=\lambda^2-x_1-x_2, \\ y_3=\lambda(x_1-x_3)-y_1. \end{cases} \qquad \begin{cases} \lambda=\dfrac{y_2-y_1}{x_2-x_1} & x_1\neq x_2, \\ \lambda=\dfrac{3x_1^2+a_4}{2y_1} & x_1=x_2. \end{cases}$$

例 1 $\mathbf{F}_{17}$ $E:\ y^2 = x^3 + 2x + 3,$ 出
全部 阶

解 $x = 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14,\ 15,\ 16,$
分 出 y.

$x = 0,\ y^2 = 3 \pmod{17},$,

$x = 1,\ y^2 = 6 \pmod{17},$,

$x = 2,\ y^2 = 15 \pmod{17},\quad y = 7,\ 8 \pmod{17},$

$x = 3,\ y^2 = 2 \pmod{17},\quad y = 6,\ 11 \pmod{17},$

$x = 4,\ y^2 = 7 \pmod{17},$,

$x = 5,\ y^2 = 2 \pmod{17},\quad y = 6,\ 11 \pmod{17},$

$x = 6,\ y^2 = 10 \pmod{17},$,

$x = 7,\ y^2 = 3 \pmod{17},$,

$$
\begin{aligned}
&x = 8,\ y^2 = 4 \pmod{17}, \quad y = 2,\ 15 \pmod{17},\\
&x = 9,\ y^2 = 2 \pmod{17}, \quad y = 6,\ 11 \pmod{17},\\
&x = 10,\ y^2 = 3 \pmod{17}, \qquad\qquad ,\\
&x = 11,\ y^2 = 13 \pmod{17}, \quad y = 8,\ 9 \pmod{17},\\
&x = 12,\ y^2 = 4 \pmod{17}, \quad y = 2,\ 15 \pmod{17},\\
&x = 13,\ y^2 = 16 \pmod{17}, \quad y = 4,\ 13 \pmod{17},\\
&x = 14,\ y^2 = 4 \pmod{17}, \quad y = 2,\ 15 \pmod{17},\\
&x = 15,\ y^2 = 8 \pmod{17}, \quad y = 5,\ 12 \pmod{17},\\
&x = 16,\ y^2 = 0 \pmod{17}, \quad y = 0 \pmod{17}.
\end{aligned}
$$

$$
\#(E(\mathbf{F}_{17})) = 1 + \sum_{x=0}^{17-1} \left(\frac{x^3 + 2x + 3}{17} \right) = 22.
$$

2 $\mathbf{F}_{17}$ $E:\ y^2 = x^3 + 2x + 3$ $P = (2, 7)$, $Q = (11, 8)$. $P + Q = (x_3, y_3),\ 2P = (x_4, y_4),\ 4P = (x_5, y_5),\ 8P = (x_6, y_6),\ 10P = (x_7, y_7),\ 11P = (x_8, y_8),\ 22P$.

令 $x_1 = 2,\ y_1 = 7, x_2 = 11,\ y_2 = 8,$ $\lambda_1 = \frac{y_2 - y_1}{x_2 - x_1} = 2,$

$$x_3 = \lambda_1^2 - x_1 - x_2 = 8, \qquad y_3 = \lambda_1(x_1 - x_3) - y_1 = 15$$

$$\lambda_2 = \frac{3x_1^2 + a_4}{2y_1} = 1,$$

$$x_4 = \lambda_2^2 - 2x_1 = 14, \qquad y_4 = \lambda_2(x_1 - x_4) - y_1 = 15$$

$$\lambda_3 = \frac{3x_4^2 + a_4}{2y_4} = 14,$$

$$x_5 = \lambda_3^2 - 2x_4 = 15, \qquad y_5 = \lambda_3(x_4 - x_5) - y_4 = 5$$

$$\lambda_4 = \frac{3x_5^2 + a_4}{2y_5} = 15,$$

$$x_6 = \lambda_4^2 - 2x_5 = 8, \qquad y_6 = \lambda_4(x_5 - x_6) - y_5 = 15$$

$$\lambda_5 = \frac{y_6 - y_4}{x_6 - x_4} = 0,$$

$$x_7 = \lambda_5^2 - x_4 - x_6 = 12, \qquad y_7 = \lambda_5(x_4 - x_7) - y_4 = 2$$

$$\lambda_6 = \frac{y_7 - y_1}{x_7 - x_1} = 8,$$

$$x_8 = \lambda_6^2 - x_1 - x_7 = 16, \qquad y_8 = \lambda_6(x_1 - x_8) - y_1 = 0$$

$11P = (x_8, y_8) = (16, 0)$ 垂 x

$22P = 2(11P) = O$ ( ).

3 $\mathbf{F}_{17}$ $E: y^2 = x^3 + 3x + 1,$

$x = 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11,\ 12,\ 13,\ 14,\ 15,\ 16,$

$y.$

$x = 0,\ y^2 = 1 \pmod{17}, \quad y = 1,\ 16 \pmod{17},$

$x = 1,\ y^2 = 5 \pmod{17}, \quad ,$

$x = 2,\ y^2 = 15 \pmod{17}, \quad y = 7,\ 8 \pmod{17},$

$x = 3,\ y^2 = 3 \pmod{17}, \quad ,$

$x = 4,\ y^2 = 9 \pmod{17}, \quad y = 3,\ 14 \pmod{17},$

$x = 5,\ y^2 = 5 \pmod{17}, \quad ,$

$x = 6,\ y^2 = 14 \pmod{17}, \quad ,$

$x = 7,\ y^2 = 8 \pmod{17}, \quad y = 5,\ 12 \pmod{17},$

$$
\begin{aligned}
&x = 8,\ y^2 = 10 \pmod{17}, && ,\\
&x = 9,\ y^2 = 9 \pmod{17}, && y = 3,\ 14 \pmod{17},\\
&x = 10,\ y^2 = 11 \pmod{17}, && ,\\
&x = 11,\ y^2 = 5 \pmod{17}, && ,\\
&x = 12,\ y^2 = 14 \pmod{17}, && ,\\
&x = 13,\ y^2 = 10 \pmod{17}, && ,\\
&x = 14,\ y^2 = 16 \pmod{17}, && y = 4,\ 13 \pmod{17},\\
&x = 15,\ y^2 = 4 \pmod{17}, && y = 2,\ 15 \pmod{17},\\
&x = 16,\ y^2 = 14 \pmod{17}, && .
\end{aligned}
$$

$$
\#(E(\mathbf{F}_{17})) = 1 + \sum_{x=0}^{17-1} \left(\frac{x^3 + 3x + 1}{17} \right) = 15.
$$

4 $\mathbf{F}_{17}$ $E: \ y^2 = x^3 + 3x + 1$ $P = (2, 7)$. $2P = (x_2, y_2),\ 3P = (x_3, y_3),\ 4P = (x_4, y_4),\ 5P = (x_5, y_5).$ $6P = (x_6, y_6),\ 7P = (x_7, y_7),\ 8P = (x_8, y_8),\ 9P = (x_9, y_9),\ 10P = (x_{10}, y_{10}),\ 11P = (x_{11}, y_{11}),\ 12P = (x_{12}, y_{12}),\ 13P = (x_{13}, y_{13}),\ 14P = (x_{14}, y_{14}).$

$$x_1 = 2,\ y_1 = 7, \qquad \lambda_2 = \frac{3x_1^2 + a_4}{2y_1} = 12,$$

$$x_2 = \lambda_2^2 - 2x_1 = 4, \qquad y_3 = \lambda_2(x_1 - x_2) - y_1 = 3$$

$$\lambda_3 = \frac{y_2 - y_1}{x_2 - x_1} = 15,$$

$$x_3 = \lambda_3^2 - x_1 - x_2 = 15, \qquad y_3 = \lambda_3(x_1 - x_3) - y_1 = 2$$

$$\lambda_4 = \frac{3x_2^2 + a_4}{2y_2} = 0,$$

$$x_4 = \lambda_4^2 - 2x_2 = 9, \qquad y_4 = \lambda_4(x_2 - x_4) - y_2 = 14$$

$$\lambda_5 = \frac{y_4 - y_1}{x_4 - x_1} = 1,$$

$$x_5 = \lambda_5^2 - x_1 - x_4 = 7, \qquad y_5 = \lambda_5(x_1 - x_5) - y_1 = 5$$

$$\lambda_6 = \frac{y_4 - y_2}{x_4 - x_2} = 9,$$

$$x_6 = \lambda_6^2 - x_2 - x_4 = 0, \qquad y_6 = \lambda_6(x_2 - x_6) - y_2 = 16$$

$$\lambda_7 = \frac{y_6 - y_1}{x_6 - x_1} = 4,$$

$$x_7 = \lambda_7^2 - x_1 - x_6 = 14, \qquad y_7 = \lambda_7(x_1 - x_7) - y_1 = 13$$

$$\lambda_8 = \frac{3x_4^2 + a_4}{2y_4} = 10,$$

$$x_8 = \lambda_8^2 - 2x_4 = 14, \qquad y_8 = \lambda_8(x_4 - x_8) - y_4 = 4$$

$$\lambda_9 = \frac{y_8 - y_1}{x_8 - x_1} = 4,$$

$$x_9 = \lambda_9^2 - x_1 - x_8 = 0, \qquad y_9 = \lambda_9(x_1 - x_9) - y_1 = 1$$

$\lambda_{10} = \frac{y_8 - y_2}{x_8 - x_2} = 12,$

$x_{10} = \lambda_{10}^2 - x_2 - x_8 = 7, \qquad y_{10} = \lambda_{10}(x_2 - x_{10}) - y_2 = 12$

$\lambda_{11} = \frac{y_{10} - y_1}{x_{10} - x_1} = 1,$

$x_{11} = \lambda_{11}^2 - x_1 - x_{10} = 9, \qquad y_{11} = \lambda_{11}(x_1 - x_{11}) - y_1 = 3$

$\lambda_{12} = \frac{y_8 - y_4}{x_8 - x_4} = 15,$

$x_{12} = \lambda_{12}^2 - x_4 - x_8 = 15, \qquad y_{12} = \lambda_{12}(x_4 - x_{12}) - y_4 = 15$

$\lambda_{13} = \frac{y_{12} - y_1}{x_{12} - x_1} = 15,$

$x_{13} = \lambda_{13}^2 - x_1 - x_{12} = 4, \qquad y_{13} = \lambda_{13}(x_1 - x_{13}) - y_1 = 14$

$\lambda_{14} = \frac{y_{12} - y_2}{x_{12} - x_2} = 15,$

$x_{14} = \lambda_{14}^2 - x_2 - x_{12} = 2, \qquad y_{14} = \lambda_{14}(x_2 - x_{14}) - y_2 = 10$

最后　$14P = -P$, $15P = O$ (　　).

$\mathbf{F}_{2^n}$ $(n \geq 1)$ E, $j(E) \neq 0$.

$\mathbf{F}_{2^n}$ 2, $\mathbf{F}_{2^n}$ E Weierstrass

$$E: \ y^2 + xy = x^3 + a_2 x^2 + a_6.$$

E $\mathbf{F}_{2^n}$

$P_1 = (x_1, y_1),\ P_2 = (x_2, y_2)$ E O

(1) $O + P_1 = P_1 + O$; (2) $-P_1 = (x_1, x_1 + y_1)$;

(3) $P_3 = (x_3, y_3) = P_1 + P_2 \neq O$,

$$\begin{cases} x_3 = \lambda^2 + \lambda + x_1 + x_2 + a_2, \\ y_3 = \lambda(x_1 + x_3) + x_3 + y_1. \end{cases}$$

$$\begin{cases} \lambda = \dfrac{y_2 + y_1}{x_2 + x_1} & x_1 \neq x_2, \\ \lambda = \dfrac{x_1^2 + y_1}{x_1} & x_1 = x_2. \end{cases}$$

$\mathbf{F}_{3^n}$ $(n \geq 1)$ E, $j(E) \neq 0$.

$\mathbf{F}_{3^n}$ 3, $\mathbf{F}_{3^n}$ E Weierstrass

$$E: \ y^2 = x^3 + a_2x^2 + a_6.$$

E $\mathbf{F}_{3^n}$

$P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$ E O

(1) $O + P_1 = P_1 + O$; (2) $-P_1 = (x_1, -y_1)$;

(3) $P_3 = (x_3, y_3) = P_1 + P_2 \neq O$,

$$\begin{cases} x_3 = \lambda^2 - x_1 - x_2 - a_2, \\ y_3 = \lambda(x_1 - x_3) - y_1. \end{cases}$$

$$\begin{cases} \lambda = \dfrac{y_2 - y_1}{x_2 - x_1} & x_1 \neq x_2, \\ \lambda = \dfrac{3x_1^2 + 2a_2x_2}{2y_1} & x_1 = x_2. \end{cases}$$

$\mathbf{K} = \mathbf{F}_q$　　$q = p^n$ 元　限　　E　　$\mathbf{F}_q$

$p > 3$　　Weierstrass

$$y^2 = x^3 + a_4 x + a_6.$$

易知　$\mathbf{F}_q$　　E　　$\#(E(\mathbf{F}_q)) \leq 2q + 1$. 事

每　$x \in \mathbf{F}_q$, 至多　　$y \in \mathbf{F}_q$ 使得 $P(x, y) \in E$, 再加

O, 我们　$\#(E) \leq 2|\mathbf{F}_q| + 1 = 2q + 1.$

$$\varphi: \begin{array}{ccc} \overline{\mathbf{F}}_q & \longrightarrow & \overline{\mathbf{F}}_q \\ (x,y) & \longmapsto & (x^q, y^q) \\ O & \longmapsto & O \end{array}$$

$\mathbf{F}_q$ E 映射

φ 叫做 q 幂 **Frobenius 映射**. φ E 映 E, 且保持群 这就 φ $\mathbf{F}_q$ E 群同态 φ 又叫做 q 幂 **Frobenius 自同态**.

Frobenius 自同态 φ 迹 (trace) 研究 起着重要作用 它 联

$$\varphi^2 - [t]\varphi + [q] = [0],$$

也就 E 任 $P = (x, y)$,

$$(x^{q^2}, y^{q^2}) - [t](x^q, y^q) + [q](x, y) = O.$$

外

$$\#(E(\mathbf{F}_q)) = q + 1 - t.$$

第 $E(\mathbf{F}_q)$ 逼近估 面 Hasse 理给

定理 1(Hasse). E $\mathbf{F}_q$ $(q = p^n,\ p$ $)$

φ q **Frobenius** E $\#(E(\mathbf{F}_q))$ 满足

$$|\#(E(\mathbf{F}_q)) - (q+1)| \leq 2\sqrt{q}.$$