



信息安全数学基础

密码学基础和数论基础

作者：熊睿 & Stander-by

组织：HUST-CSE-2004

时间：Mar 7, 2022

版本：1.0



学习新思想，争做新青年。

特别声明

该笔记是于 2022 年 3 月 7 日开始，针对华中科技大学网络安全学院 2020 级信息安全数学基础课程编制的笔记，该课程使用的是 HUST-CSE 汤学明老师所著的《信息安全数学基础》，还有中国科学院大学的陈恭亮老师所编著的《信息安全数学基础》，陈恭亮老师也是汤老师在 WHU 读研的导师。学有余力时，还应去翻阅华罗庚的著作《数论引导》。

该课程所运用的主要编程环境是开源的 SageMath，同时根据需要可以使用 python 和 mathematical 等。

SageMath-GitHub 网址：<https://github.com/sagemath/>

该课程前有《离散数学》打基础，后为《密码学原理》铺路，是理论与实践之间的桥梁，理解抽象知识，提高解决实际数学、密码学问题的能力。

同时使用优美的 \LaTeX 来书写，也少不了 WHU 好友的鼎力推荐 (Thanks)，也希望能通过这次机会，去熟悉 \LaTeX 的语法，特别是数学公式的编写，和作图能力。

另外，“多分享，多奉献”，之后我会将文档同步于我的 Github 账号，由于编者的水平有限，会存在一些难免的疏漏和问题，请大家批评指正！

我的 GitHub 网址：<https://github.com/Stander-by/>

我的邮件：xiongruistanderby@gmail.com

NodeBB 校内网：<http://10.12.162.1:5881/>

NodeBB 校外网：<http://124.71.166.97:5881/>

SageMath:<http://10.12.162.1:5883/>

Stander-by
Mar 7, 2022

目录

1	整除	1
1.1	整除性	1
1.2	欧几里得辗转相除法	2
1.3	一次不定方程	3
1.4	最小公倍数	5
1.5	素数与算术基本定理	6
1.6	高斯函数	7
	第 1 章 练习	8
2	同余	10
2.1	同余的基本性质	10
2.2	欧拉函数	12
2.2.1	剩余系的遍历	12
2.2.2	欧拉函数	12
2.3	欧拉定理	14
2.3.1	欧拉定理和费马定理	14
2.3.2	扩展欧拉定理	14
2.3.3	模重复平方算法	15
2.4	一次同余式	15
2.4.1	同余式及其解数	15
2.4.2	一次同余式	16
2.4.3	逆元	16
2.5	中国剩余定理	17
2.5.1	中国剩余定理	17
2.5.2	递推法	18
2.5.3	应用	19
2.6	同余式组解法	19
2.6.1	同余式组解数	19
2.6.2	模同一素数幂	20
2.6.3	一般同余式求解	21
2.7	模为素数幂的高层同余式	21
2.8	高次同余式求解方法	22
2.8.1	唯一解	22
2.8.2	无解	22
2.8.3	多个解	22
2.8.4	复杂情况	23
	第 2 章 练习	23
3	域	25
3.1	域的定义与性质	25
3.1.1	域的定义	25
3.1.2	子域和扩域	25

3.2	域的特征	26
3.2.1	特征的定义	26
3.2.2	域的同构	26
3.2.3	素域	26
3.3	二项式定理	27
3.3.1	二项式定理	27
3.3.2	特征幂的二项式定理	27
3.3.3	域上的多项式	27
3.3.4	多项式的加法和乘法	27
3.4	多项式的辗转相除法	28
3.4.1	带余除法算式	28
3.4.2	因式与倍式	29
3.4.3	辗转相除法	29
3.5	多项式整除和唯一因式分解定理	29
3.5.1	多项式整除的性质	29
3.5.2	多项式的模逆	30
3.5.3	唯一因式分解定理	30
3.6	扩域的构造	31
3.6.1	多项式的根	31
3.6.2	扩域的构造	31
3.7	有限域的乘法群	31
3.7.1	有限域的乘法群	31
3.7.2	循环群的结构	31
4		33
4.1	勒让德符号	33
4.1.1	欧拉判别法则	33

第1章 整除

第一章讲述整数整除中带余除法、因子、最大公因数、最小公倍数和算术基本定理等基本概念，希望通过从带余除法到最终的算术基本定理的推导过程，掌握整数研究的一般方法，在第三章多项式的唯一因式分解定理的推到过程中，用到这种系统化的方法。

1.1 整除性

定理 1.1 (带余除法)

任意给定整数 a 和整数 $b > 0$ ，存在唯一的一对整数 q ， $0 \leq r < b$ ，使得： $a = qb + r$ 。



推论 1.1

任意给定整数 a 和整数 $b < 0$ ，存在唯一的一对整数 q ， $0 \leq r < |b|$ ，使得： $a = qb + r$ 。



推论 1.2

任意给定整数 a ， c 和整数 $b \neq 0$ ，存在唯一的一对整数 q ， $c \leq r < |b| + c$ ，使得 $a = qb + r$ 。



定理 1.2 (整除性质)

设 a ， b ， c 为整数

- (1) 若 $a \mid b$ ， $b \mid a$ ，则 $a = \pm b$ ；
- (2) 设整数 $k \neq 0$ ，若 $a \mid b$ ，则 $\pm ka \mid \pm kb$ ，反之亦然；
- (3) 对任意整数 k ，若 $a \mid b$ ，则 $a \mid kb$ ；
- (4) 若 $a \mid b$ ， $b \neq 0$ ，则 $\frac{b}{a} \mid b$ ；
- (5) 若 $a \mid b$ ， $b \mid c$ ，则 $a \mid c$ ；
- (6) 若 $a \mid b$ ， $a \mid c$ ，则对任意整数 s 和 t ， $a \mid sb + tc$ ；



例题 1.1 若 a 是整数，证明 $a^3 - a$ 是 6 的倍数。

证明

$$a^3 - a = (a - 1)a(a + 1)$$

由定理 1.2 之 (3) 有， $3 \mid (a - 1)a(a + 1)$ ，可设 $(a - 1)a(a + 1) = 3q$ 。

同理，因为两个连续的整数中一定有一个是 2 的倍数，所以 $2 \mid (a - 1)a(a + 1)$ ，不妨设 $q = 2t$ ，于是 $(a - 1)a(a + 1) = 6t$ ，根据整除的定义， $6 \mid (a - 1)a(a + 1)$ 。

例题 1.2 若 x ， y 为整数，证明： $10 \mid 2x + 5y \Leftrightarrow 10 \mid 4x + 5y$ 。

证明

由定理 1.2 之 (4) 有

$$4x + 5y = 10(x + 2y) - 3(2x + 5y)$$

$$2x + 5y = 3(4x + 5y) - 10(x + y)$$

练习 1.1

- 1) 是否存在 n ，使得 $n + 1 \mid n!$ ？
- 2) 如果 $n \mid x^2 - y^2$ ，那么 $n \mid x + y$ 或者 $n \mid x - y$ 是否成立？



笔记

1.2 欧几里得辗转相除法

定义 1.1

(a, b) $\gcd(a, b)$ 表示为 a 和 b 的最大公因数。



定理 1.3

设 a, b 是两个不全为 0 的整数, 且 $a = qb + r$, r 为整数, 则 $(a, b) = (b, r)$ 。



证明

设 $d = (a, b)$ $d' = (b, r)$

由定理 1.2 (6) 得, $d \mid (a - qb)$ 即 $d \mid r$

且 $d \leq d'$, 所以 $d = d'$ 。

推论 1.3

设 a, b 是两个不全为 0 的整数, q 为整数, 则 $(a, b) = (a \pm bq, b) = (a, b \pm aq)$ 。



例题 1.3 证明: 若 n 为整数, 则 $(21n + 4, 14n + 3) = 1$, $(n^3 + 2n, n^4 + 3n^2 + 1) = 1$ 。

定理 1.4 (辗转相除法)

设 a, b 是两个正整数, 下式为起欧几里得辗转相除算式

令 $r_0 = a$ $r_1 = b$, 反复运用带余除法算式:

$$\begin{array}{ll} r_0 = r_1 q_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 = r_2 q_2 + r_3 & 0 \leq r_3 < r_2 \\ \vdots & \vdots \\ r_{n-2} = r_{n-1} q_{n-1} + r_n & 0 \leq r_n < r_{n-1} \\ r_{n-1} = r_n q_n + r_{n+1} & r_{n+1} = 0 \end{array}$$

由于 $r_{n+1} < r_n < r_{n-1} < \dots < r_2 < r_1 = b$, 且 b 为有限正整数, 所以经过有限的正整数, 所以经过有限的步骤, 必然存在 n , 使得 $r_{n+1} = 0$ 。

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

(2) 存在整数 s, t , 使得 $r_n = sa + tb$

(3) 任意整数 c , 若满足 $c \mid a$ 且 $c \mid b$, 则 $c \mid r_n$



定理 1.5

设 a, b 是两个正整数, q_i 为其欧几里得辗转相除算式的部分商, 则由

$$\begin{aligned} S_0 &= 0 \\ S_1 &= 1 \\ S_{i+1} &= S_{i-1} - q_{n-i} S_i \quad i \geq 1 \end{aligned}$$

所得的 S_{n-1} 和 S_n 满足 $S_{n-1}a + S_nb = r_n$ 。

$$\begin{pmatrix} r_1 \\ r_2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_1 \end{pmatrix} \begin{pmatrix} r_0 \\ r_1 \end{pmatrix}$$

$$\begin{pmatrix} r_2 \\ r_3 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_2 \end{pmatrix} \begin{pmatrix} r_1 \\ r_2 \end{pmatrix}$$

$$\dots\dots\dots$$

$$\begin{pmatrix} r_{n-1} \\ r_n \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & -q_{n-1} \end{pmatrix} \begin{pmatrix} r_{n-2} \\ r_{n-1} \end{pmatrix}$$



例题 1.4 试求 s, t , 使得 $30111s + 4520t = (30111, 4520)$ 。

解

i	0	1	2	3	4	5	6	7	8	9	10	11
q_{12-i}			2	1	1	4	1	21	1	1	1	6
S_i	0	1	-2	3	-5	23	-28	611	-639	1250	-1889	12584



笔记 $S_{i+1} = S_{i-1} - q_{n-i}S_i$



练习 1.2

- 1) 如果 $(a, b) = d$, 那么 $\{sa + tb \mid s, t \in \mathbb{Z}\}$ 是什么?
- 2) 试求出一对整数 s 和 t 满足 $s * 12345 - t * 345 = (12345, 345)$ 。

1.3 一次不定方程

定理 1.6

设 a, b 是两个不全为 0 的整数, 则

- (1) 对于任何正整数 k , $(ka, kb) = k(a, b)$
- (2) $(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$



证明 (2) 由 (1), $(a, b)(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = ((a, b)\frac{a}{(a,b)}, (a, b)\frac{b}{(a,b)}) = (a, b)$
 因为 $(a, b) \neq 0$, 所以 $(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$ 。

定理 1.7

设 a, b, c 为整数, $a \neq 0, c \neq 0$, 若 $(a, b) = 1$, 则 $(a, bc) = (a, c)$ 。



注 $d = (a, bc), d' = (a, c)$ proof $d \mid d'$ and $d' \mid d$ 。

推论 1.4

设 a, b, c 为整数, $a \neq 0$, 若 $(a, b) = 1, a \mid bc$, 则 $a \mid c$ 。



例题 1.5 证明: 若 $a_1b_1 - a_2b_2 = 1$, 则 $(a_1 + a_2, b_1 + b_2) = 1$ 。

证明 $a_1b_1 - a_2b_2 = 1 \Rightarrow (b_1, b_2) = 1, (a_1, a_2) = 1$ comes from 1.2(6)

$$(b_1, b_1 + b_2) = (b_1, b_2) = 1$$

$$(b_1 + b_2, b_1(a_1 + a_2)) = (b_1 + b_2, a_1 + a_2)$$

$$(b_1 + b_2, b_1(a_1 + a_2)) = (b_1 + b_2, b_1(a_1 + a_2) - a_2(b_1 + b_2)) = (b_1 + b_2, 1) = 1。$$

定理 1.8

设 a, b 是两个完全不为 0 的整数, 整系数不定方程 $ax + by = c$ 有解的充分条件是 $(a, b) = c$ 。此时, 若 $x = x_0, y = y_0$ 是方程的一个特解, 那么方程的所有整数解可以表示为:

$$\begin{cases} x = x_0 - \frac{b}{(a, b)}t \\ y = y_0 + \frac{a}{(a, b)}t \\ t \in Z \end{cases}$$



例题 1.6 求不定方程 $18x + 7y = 44$ 的所有整数解

解 根据辗转相除法可得

$18 * 2 + 7 * (-5) = 1$ 特解为:

$$\begin{cases} x = 2 \\ y = -5 \end{cases}$$

不定方程 $18x + 7y = 44$ 的特解为:

$$\begin{cases} x_0 = 2 \times 44 = 88 \\ y_0 = (-5) \times 44 = -220 \end{cases}$$

原不定方程的特解为:

$$\begin{cases} x = 88 - 7t \\ y = -220 + 18t \\ t \in Z \end{cases}$$

例题 1.7

1. 求不定方程 $a_1x_1 + a_2x_2 + \dots + a_{n-1}x_{n-1} + x_n = N$ 的所有整数解。

2. 求不定方程 $18x + 7y + 6z = 44$ 的所有整数解。

3. 求不定方程 $6x + 10y + 15z = 44$ 的所有整数解。

解

2. $(18, 7) = 1 \Rightarrow 18x + 7y$ 可以表示任何整数, z 可以任取。

转化为 $18x + 7y = 44 - 6z$ 来求得二元不定方程的解。

3. $(6, 10) = 2 \Rightarrow 6x + 10y = 2t$


原方程转化为 $2t + 15z = 44$

其解为:

$$\begin{cases} t = -308 - 15t_1 \\ z = 44 + 2t_1 \\ t_1 \in Z \end{cases}$$

$3x + 5y = t$ 的所有整数解可以表示为;

$$\begin{cases} x = 2t - 5t_2 \\ y = -t + 3t_2 \\ t_2 \in Z \end{cases}$$

 **练习 1.3** 求解不定方程 $x^2 + y^2 = z^2$

1.4 最小公倍数

定义 1.2

设 a, b 是两个不全为 0 的整数, 整数满足 $a | c, b | c$, 则称 c 为 a 和 b 的公倍数, 在 a 和 b 的所有公倍数中, 一定有一个正的最小公倍数, 称为 a 和 b 的最小公倍数, 记作 $[a, b]$, 或者 $\text{lcm}(a, b)$ 。



定理 1.9

设 a, b 是两个正整数, 且 $(a, b) = 1$,

- (1) 若 $a | c, b | c$, 则 $ab | c$
- (2) $[a, b] = ab$



定理 1.10

设 a, b 是两个正整数,

- (1) 对于任何正整数 k , $[ka, kb] = k[a, b]$
- (2) $[a, b] = \frac{ab}{(a, b)}$
- (3) 若 $a | c, b | c$, 则 $[a, b] | c$



例题 1.8 若 $x, y, \sqrt{x} + \sqrt{y}$ 均为整数, 试证明 \sqrt{x}, \sqrt{y} 均为整数。

证明 若 $\sqrt{x} + \sqrt{y} = 0$, 则 $x = y = 0$, 结论成立

$\sqrt{x} = \frac{1}{2}((\sqrt{x} + \sqrt{y}) + (\sqrt{x} - \sqrt{y}))$ 所有 \sqrt{x}, \sqrt{y} 都是有理数

不妨设 $\sqrt{x} = \frac{b}{a}$, a, b 为正整数, 且 $(a, b) = 1$

$x = \frac{b^2}{a^2}$ 为整数, $(a^2, b^2) = a^2 \Rightarrow (a, b) = (a, b^2) = (a^2, b^2)$

所以 $a = 1$, \sqrt{x} 为整数。

定理 1.11

a_1, a_2, \dots, a_n 不全为 0 的整数, 不妨设 $a_1 \neq 0$, 定义 $d_1 = (a_1, a_2), d_2 = (d_1, a_3), \dots, d_{n-1} = (d_{n-2}, a_n)$, 则 $(a_1, a_2, \dots, a_n) = d_{n-1}$ 。



结论 若正整数 $d = (a_1, a_2, \dots, a_n)$, 则存在整数 s_1, s_2, \dots, s_n , 使得 $d = s_1 a_1 + s_2 a_2 + \dots + s_n a_n$

定理 1.12

正整数 c 是 a_1, a_2, \dots, a_n 的最大公因数, 当且仅当:

- (1) $c | a_1, c | a_2, \dots, c | a_n$ 。
- (2) 任何整数 c' 若满足 $c' | a_1, c' | a_2, \dots, c' | a_n$, 则 $c' | c$ 。



定理 1.13

设 a_1, a_2, \dots, a_n 是 n 个不为 0 的整数, 定义 $m_1 = [a_1, a_2], m_2 = [m_1, a_3], \dots, m_{n-1} = [m_{n-2}, a_n]$, 则 $[a_1, a_2, \dots, a_n] = m_{n-1}$ 。



定理 1.14

正整数 m 是 a_1, a_2, \dots, a_n 的最大公因数, 当且仅当:

- (1) $a_1 | m, a_2 | m, \dots, a_n | m$ 。
- (2) 任何整数 m' 若满足 $a_1 | m', a_2 | m', \dots, a_n | m'$, 则 $m | m'$ 。



1.5 素数与算术基本定理

定义 1.3

设 p 是一个整数, $p \neq 0, \pm 1$, 如果除了 $\pm 1, \pm p$ 外, p 没有其他因数, 则称 p 为素数 (或者质数, 不可约数), 否则为合数 (可约数), 最小的素数为 2.



定理 1.15

合数 m 的最小不等于 1 的正因子 p 一定是素数, 且 $p \leq \sqrt{m}$.



证明 反证法证明 p 一定是素数。

由 1.2 (4) $\Rightarrow \frac{m}{p} \mid m$, 又 $1 < \frac{m}{p} < m$, $p \leq \frac{m}{p} \Rightarrow p \leq \sqrt{m}$.

结论 设整数 $m > 1$, 如果所有不大于 \sqrt{m} 的素数都不是 m 的因子, 那么 m 是素数。

整数 $m > 1$ 是合数的充要条件是存在不大于 \sqrt{m} 的素因子。

定理 1.16

素数有无穷多个。



证明 反证法证明, 有有限个素数 p_1, p_2, \dots, p_n

考虑整数 $A = p_1 p_2 \dots p_n + 1$

不妨设 $p_i \mid A \Rightarrow p_i \mid A - p_1 p_2 \dots p_n$, 即 $p_i \mid 1$, 矛盾。

定理 1.17 (素数定理)

$\pi(x)$ 表示不超过 x 的素数个数。

$$\lim_{x \rightarrow \infty} \pi(x) \frac{\ln(x)}{x} = 1$$



定理 1.18 (伯特兰-切比雪夫定理)

设整数 $n > 3$, 至少存在一个素数 p 满足 $n < p < 2n - 2$.



定理 1.19 (算术基本定理)

设 n 是一个大于 1 的正整数, 那么 n 一定可以分解成一些素数的乘积。若规定 n 的所有素因子按照从小到大的顺序排列, 那么 n 的分解方式是唯一的。



定义 1.4

设 n 是大于 1 的正整数, $n = \prod_{i=1}^s p_i^{\alpha_i} (\alpha_i > 0, p_i < p_j (i < j))$ 称为 n 的标准分解式。



例题 1.9 设 $m = \prod_{i=1}^s p_i^{\alpha_i}$, $n = \prod_{i=1}^s p_i^{\beta_i}$, $\alpha_i \geq 0, \beta_i \geq 0, p_i \neq p_j (i \neq j)$ proof:

$$(1) m \mid n \Leftrightarrow 1 \leq i \leq s, \alpha_i \leq \beta_i$$

$$(2) (m, n) = \prod_{i=1}^s p_i^{\min \alpha_i, \beta_i}$$

$$(3) [m, n] = \prod_{i=1}^s p_i^{\max \alpha_i, \beta_i}$$

练习 1.4 证明形如 $4k + 3$ 的素数有无穷多个。

证明 反证法证明, 假设形如 $4k + 3$ 素数仅有有限个, 其全部为 p_1, p_2, \dots, p_n , 均为大于 1 的正整数, 考虑整奇

数: $A = 4p_1p_2 \dots p_n - 1$

A 是一个形如 $4k + 3$ 的合数

所以 A 的素因子全部都是形如 $4k + 1$ 的素数, 但形如 $4k + 1$ 的整数相乘仍然是形如 $4k + 1$ 的整数, 矛盾。

练习 1.5

1. 试证明: $\max\{a, b, c\} = a + b + c + \min\{a, b, c\} - \min\{a, b\} - \min\{b, c\} - \min\{a, c\}$
2. 试证明: $\gcd(a, \text{lcm}(b, c)) = \text{lcm}(\gcd(a, b), \gcd(a, c))$
3. 试用算术基本定理证明:

$$\prod_p \frac{p}{p-1} = \sum_{i=1}^{+\infty} \frac{1}{i}$$

1.6 高斯函数

定义 1.5

实数 x 的高斯函数 $[x]$ 是指不超过 x 的最大的整数, $[x]$ 也称为 x 的整数部分, x 的小数部分 x 是指 $x - [x]$ 。

定理 1.20

对于 $[x]$, 以下结论正确:

1. 若 $x \leq y \Rightarrow [x] \leq [y]$
2. 整数 a 满足 $x - 1 < a \leq x + 1 \Leftrightarrow a = [x]$
3. 整数 a 满足 $a \leq x < a + 1 \Leftrightarrow a = [x]$
4. 对于任意整数 n , $[n + x] = n + [x]$

证明 (4)

$$n + x - 1 < [n + x] \leq n + x$$

$$x - 1 < [n + x] - n \leq x$$

$$[n + x] - n = [x]$$

例题 1.10 对于任意实数 x, y , 试证明 $[x + y] \geq [x] + [y]$

证明

$$[x + y] = [[x] + [y] + \{x\} + \{y\}]$$

$$[x + y] = [x] + [y] + [\{x\} + \{y\}]$$

$$[\{x\} + \{y\}] \geq 0$$

$$[x + y] \geq [x] + [y]$$

定理 1.21

对于整数 a, b , 且 $b > 0$, 带余除法算式为 $a = qb + r, 0 \leq r < b$, 则 $q = [\frac{a}{b}]$ 。

证明

$$q = \frac{a}{b} - \frac{r}{b}, \quad 0 \leq \frac{r}{b} < 1$$

$$\frac{a}{b} - 1 \leq q = \frac{a}{b} - \frac{r}{b} < \frac{a}{b}$$

定理 1.22

设 p 是一个素数, 则 $n!$ 中包含 p 的幂次为 $\sum_{i \geq 1} [\frac{n}{p^i}]$ 。

for example:

$$\begin{aligned} 30! &= 1 \times 2 \times \cdots \times 30 = p_1^{e_1} p_2^{e_2} \cdots = 2^{e_1} 3^{e_2} \cdots \\ &= \left[\frac{30}{2}\right] + \left[\frac{30}{2^2}\right] + \left[\frac{30}{2^3}\right] + \left[\frac{30}{2^4}\right] + \left[\frac{30}{2^5}\right] \cdots \\ &= 15 + 7 + 3 + 1 + 0 + \cdots \end{aligned}$$

所以 $e_1 = 15 + 7 + 3 + 1$

证明 定理 1.22

p^i 的倍数共有 $\left[\frac{n}{p^i}\right]$

当 $(p, k) = 1$ 时, 整数 $p^i k$ 为 $n!$ 提供的 p 的幂次为 i

由于 $p^i k$ 同时是 p, p^2, \dots, p^i 的倍数, 所以恰好共计数了 i 次

因此 $n!$ 中包含 p 的幂次为 $\sum_{i \geq 1} \left[\frac{n}{p^i}\right]$

例题 1.11 试证明 $\binom{100}{50}$ 的十进制末位数不为 0.

证明

$$\binom{100}{50} = \frac{100!}{50!50!}$$

$$100! = 2^{e_1} 3^{e_2} 5^{e_3} \cdots$$

$$50! = 2^{b_1} 3^{b_2} 5^{b_3} \cdots$$

$$b_3 = \left[\frac{50}{5}\right] + \left[\frac{50}{25}\right] + \left[\frac{50}{125}\right]$$

$$e_3 = \left[\frac{100}{5}\right] + \left[\frac{100}{25}\right] + \left[\frac{100}{125}\right]$$

所以 $\binom{100}{50}$ 没有素因数 5, 所以末位不为 0.

例题 1.12 设 n, m 为正整数, $n > m$, 试证明: $\binom{n}{m} = \frac{n(n-1)\cdots(n-m+1)}{m!}$ 是整数。

证明

$$\binom{n}{m} = \frac{n!}{m!(n-m)!}$$

只需证明 $\sum_{i \geq 1} \left[\frac{n}{p_i}\right] \geq \sum_{i \geq 1} \left[\frac{m}{p_i}\right] + \sum_{i \geq 1} \left[\frac{n-m}{p_i}\right]$

由例题 1.10 可知 $\left[\frac{n}{p_i}\right] \geq \left[\frac{m}{p_i}\right] + \left[\frac{n-m}{p_i}\right]$

第1章 练习

1. 设 a, m, n 均为正整数, 试着证明 $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$

证明 *Might as well, $m \geq n, m = nq + r, 0 \leq r < n$*

$$a^m - 1 = a^{nq+r} - a^r + a^r - 1 = a^r(a^{nq} - 1) + a^r - 1$$

$$= a^r(a^n - 1)(1 + a^n + a^{2n} + \cdots + a^{(q-1)n}) + a^r - 1$$

so $(a^m - 1) \bmod (a^n - 1) = a^r - 1$

using division algorithm, the answer is $a^{(m,n)} - 1$.

2. The Fermat number is $F_n = 2^{2^n} + 1$, if F_n is prime number, try to proof :
if $2^m + 1$ is prime number then m just like $2^n \in \mathbb{Z}$.

证明

第2章 同余

2.1 同余的基本性质

定义 2.1

设 m 是正数, a, b 为两个整数, 如果 $a-b$ 是 m 的倍数, 那么称 a 和 b 关于 m 同余, 记作 $a \equiv b(\text{mod } m)$, 否则称 a 和 b 关于 m 不同余, 记作 $a \not\equiv b(\text{mod } m)$ 。

定理 2.1

同余式等价关系

1. 自反性
2. 对称性
3. 传递性

定义 2.2

设 m 是正整数, 全体整数按照模 m 同余可以划分成 m 个不同的等价类, 称为模 m 剩余类, 整数 a 所在的剩余类记为 \bar{a} , 整数 x 属于剩余类 \bar{a} 当且仅当 $x \equiv a(\text{mod } m)$ 。从每个剩余类中取出一个整数形成的 m 元素称为模 m 完全剩余系。

例如, 若 $m=6$, 则模 6 剩余类共有 6 个可以表示为 $\bar{0}, \bar{1}, \bar{2}, \dots, \bar{5}$ 而 $0, 1, 2, 3, 4, 5, -6, 7, 2, 3, 4, 5$ 都是模 6 完全剩余系。

定义 2.3

设 m 是正整数, 如果整数 a 与 m 互素, 那么 a 所在的剩余类 \bar{a} 称为模 m 简化剩余类, 从每个简化剩余类中取出一个整数形成的集合称为模 m 的简化剩余系。在整数 $1, 2, \dots, m$ 中所有与 m 互素的整数的个数称为 m 的欧拉函数, 记作 $\varphi(m)$, 简化剩余系共有 $\varphi(m)$ 个整数。


例题 2.1 设 m, n 为正整数, 试将模 m 的剩余类 \bar{a} 拆分成模 mn 的剩余类的和。

解

- 模 m 剩余类 $a(\text{mod } m)$ 可以表示为 $\{a + mk | k \in \mathbb{Z}\}$, 而全体整数按照模 n 又可以分成 n 个剩余类, 即 $\bar{0}, \bar{1}, \dots, \bar{n-1}$ 。
- $\{a + mk | k \in \mathbb{Z}\} = \{a + m(tn) | t \in \mathbb{Z}\} \cup \{a + m(tn+1) | t \in \mathbb{Z}\} \cup \dots \cup \{a + m(tn+n-1) | t \in \mathbb{Z}\}$ 。
- $= \{a + mnk | t \in \mathbb{Z}\} \cup \{a + m + mnt | t \in \mathbb{Z}\} \cup \dots \cup \{a + m(n-1) + mnt | t \in \mathbb{Z}\}$
- 也就是, 模 m 的剩余类 \bar{a} 可以拆分成 n 个模 mn 的剩余类, $\bar{a}, \overline{a+m}, \dots, \overline{a+m(n-1)}$ 。

定理 2.2 (同余的性质)

设 m, n 是正整数, $a \equiv b(\text{mod } mn)$, 则 $a \equiv b(\text{mod } m), a \equiv b(\text{mod } n)$ 。

 **笔记** 定理 2.2 的逆定理不成立

定理 2.3

设 m, n 是正整数, 若 $a \equiv b(\text{mod } n), a \equiv b(\text{mod } m)$, 则 $a \equiv b(\text{mod } [m, n])$ 。

定理 2.4

关于同余，以下性质成立。

- (1) 若 $a \equiv b \pmod{m} \Rightarrow a + c \equiv b + c \pmod{m}$ 。
- (2) 若 $a \equiv b \pmod{m}, k \in \mathbb{Z} \Rightarrow ak \equiv bk \pmod{m}$ 。
- (3) 若 $ak \equiv bk \pmod{m}, k \in \mathbb{Z}, (k, m) = 1 \Rightarrow a \equiv b \pmod{m}$ 。
- (4) 若 $a \equiv b \pmod{m}, k \in \mathbb{Z}^+ \Leftrightarrow ak \equiv bk \pmod{mk}$ 。
- (5) 若 $a \equiv b \pmod{m}$ ， $f(x)$ 为任一整系数多项式，则 $f(a) \equiv f(b) \pmod{m}$ 。



结论 若 $a_1 \equiv a_2 \pmod{m}, b_1 \equiv b_2 \pmod{m} \Rightarrow a_1 + b_1 \equiv a_2 + b_2 \pmod{m}, a_1 b_1 \equiv a_2 b_2 \pmod{m}$ 。

例题 2.2 试证明正整数 m 能被 3 整除的充要条件是它的十进制表示各数位上数字之和是 3 的倍数。

证明 $m = (a_{n-1} \cdots a_1 a_0)_{10}$

$$\sum_{i=0}^{n-1} a_i 10^i \equiv \sum_{i=0}^{n-1} a_i 1^i$$

$$m \pmod{3} = \sum_{i=0}^{n-1} a_i \pmod{3}$$



笔记 讨论 9, 7, 11, 1001, 13

- $\sum_{i=0}^{n-1} a_i 10^i \equiv \sum_{i=0}^{n-1} a_i 1^i = \sum_{i=0}^{n-1} a_i \pmod{9}$
- $\sum_{i=0}^{n-1} a_i 10^i \equiv \sum_{i=0}^{n-1} a_i (-1)^i \pmod{11}$
- $12345678 = 12 \times (10^3)^2 + 345 \times 10^3 + 678$
 $= 12 \times (-1)^2 + 345 \times (-1) + 678 \pmod{1001}$
- $1001 = 7 \times 11 \times 13$

练习 2.1

1. 若 x, y 为整数，证明 $10|2x + 5y \Leftrightarrow 10|4x + 5y$ 。

解

$$10|2x + 5y \Leftrightarrow 2|2x + 5y, 5|2x + 5y.$$

$$\begin{cases} 2x + 5y \equiv 0 \pmod{2} \\ 2x + 5y \equiv 0 \pmod{5} \end{cases} \Leftrightarrow \begin{cases} y \equiv 0 \pmod{2} \\ 2x \equiv 0 \pmod{5} \end{cases} \quad (2, 5) = 1 \Leftrightarrow \begin{cases} y \equiv 0 \pmod{2} \\ x \equiv 0 \pmod{5} \end{cases}$$

$$\begin{cases} 4x + 5y \equiv 0 \pmod{2} \\ 4x + 5y \equiv 0 \pmod{5} \end{cases} \Leftrightarrow \begin{cases} x \equiv 0 \pmod{2} \\ y \equiv 0 \pmod{5} \end{cases}$$

2. 计算 $2^{1024} \pmod{10240}$

解

$$\text{考虑 } 2^{1024} \equiv x \pmod{10240} \Rightarrow 2^{1013} \equiv y \pmod{5}$$

$$\begin{aligned} 2^{1013} &= 2 \times 2^{1012} \\ &= 2(2^2)^{506} \\ &\equiv 2(-1)^{506} \end{aligned}$$

$$\text{所以 } 2^{1013} \equiv 2 \pmod{5}$$

2.2 欧拉函数

2.2.1 剩余系的遍历

定理 2.5

设 m 是正整数, 若 $(a, m) = 1$, 则当 x 遍历模 m 的一个完全剩余系时, 对于任意整数 b , $ax + b$ 遍历模 m 的一个完全剩余系; 当 x 遍历模 m 的一个简化剩余系, ax 遍历模 m 的一个简化剩余系。



证明 m 的剩余系为 $\{x_1, x_2, \dots, x_m\}$

不妨设 $1 \leq i \leq j \leq m$

$$ax_i + b \equiv ax_j + b \pmod{m} \Rightarrow x_i \equiv x_j \pmod{m}$$

矛盾

ax_i 与 m 互素, 且两两互不同余。

定理 2.6

设 m, n 为正整数, $(m, n) = 1$, 则当 x 遍历模 m 的一个完全剩余系, y 遍历模 n 的一个完全剩余系时, $mx + ny$ 遍历模 mn 的一个完全剩余系; 当 x 遍历模 m 的一个简化剩余系, y 遍历模 n 的一个简化剩余系时, $mx + ny$ 遍历模 mn 的一个简化剩余系。



证明 (x_i, y_j) 一共有 mn 种取法

$i = j$ 取法相同, $i \neq j$ 取法不同

$$mx_i + ny_j \equiv mx_{i'} + ny_{j'} \pmod{mn}$$

$$\Rightarrow y_j \equiv y_{j'} \pmod{n}$$

$$\text{proof: } (x_i, n) = 1, (y_j, m) = 1 \Rightarrow (mx_i + ny_j, mn) = 1$$

$$(mx_i + ny_j, m) = 1, (mx_i + ny_j, n) = 1$$

$\varphi(m)\varphi(n)$ 个元素和 mn 互素

$$\varphi(m)\varphi(n) \leq \varphi(mn)$$

证明 $\varphi(mn)$ 无遗漏

当 x 遍历完全, y 遍历完全, $mx + ny$ 遍历完全

$$\forall a \in \mathbb{Z}, \exists x_i, y_j \Rightarrow a \equiv mx_i + ny_j \pmod{mn}$$

$$(a, mn) = 1 \Rightarrow \begin{cases} (a, m) = 1 \\ (a, n) = 1 \end{cases} \Rightarrow \begin{cases} (mx_i + ny_j, m) = 1 \\ (mx_i + ny_j, n) = 1 \end{cases} \Rightarrow \begin{cases} (y_j, m) = 1 \\ (x_i, n) = 1 \end{cases}$$

2.2.2 欧拉函数

定理 2.7

设 m, n 为正整数, 若 $(m, n) = 1$, 则 $\varphi(mn) = \varphi(m)\varphi(n)$ [积性函数]。



证明

由定理 2.6, 当 x 遍历模 n 的一个简化剩余系, y 遍历模 m 的一个简化剩余系时, $mx + ny$ 遍历模 mn 的一个简化剩余系, 所以模 mn 的一个简化剩余系中的元素个数为 $\varphi(mn) = \varphi(m)\varphi(n)$ 。

定理 2.8

设 p 为素数, e 为正整数, 则 $\varphi(p^e) = p^e - p^{e-1}$ 。



证明

p 是素数 $\varphi(p) = p - 1(1, 2, \dots, p - 1)$

$\varphi(p^e)$ 不互素的有 $p, p^2, \dots, p^{e-1}, p^e$

$$\varphi(p^e) = p^e - p^{e-1}$$

定理 2.9

设 m 为正整数, 其标准分解式为 $m = \prod_{i=0}^s p_i^{\alpha_i}$, 则 $\varphi(m) = m \prod_{i=0}^s (1 - \frac{1}{p_i})$



证明 由定理 2.7 和定理 2.8,

$$\varphi(m) = \prod_{i=1}^s \varphi(p_i^{\alpha_i}) = \prod_{i=1}^s (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = \prod_{i=1}^s p_i^{\alpha_i} (1 - \frac{1}{p_i}) = m \prod_{i=1}^s (1 - \frac{1}{p_i}).$$

例题 2.3 试求 $\varphi(2^3 3^2 7)$

解

$$\varphi(2^3 3^2 7) = 2^3 3^2 7 \times (1 - \frac{1}{2})(1 - \frac{1}{3})(1 - \frac{1}{7}) = 144$$

例题 2.4 假设 m 是两个不相等的素数的乘积, 如果已知 $\varphi(m) = a$, 试求这两个素数。

解

由题意可设 $m = pq$, p, q 为不相等的素数, 可得二元二次方程组,

$$\begin{cases} m = pq \\ (p-1)(q-1) = a \end{cases}$$

整理可得 $p + q = m + 1 - a$, 因此 p, q 为以下一元二次方程的两个解

$$x^2 - (m + 1 - a)x + m = 0$$

练习 2.2

1. 证明 $m > 2, 2|\varphi(m)$

证明

方法一:

$$\varphi(m) = \prod (p_i^{\alpha_i} - p_i^{\alpha_i-1})$$

分为两种情况考虑:

1. m 含有至少一个奇数因子

2. m 就是等于 $2^i, i > 1$

方法二:

m 为奇数

$$1, 2, 3, \dots, \frac{m-1}{2}, \frac{m+1}{2}, \dots, m$$

$$(i, m) = 1 \Rightarrow (m - i, m) = 1$$

2. 证明, 当 $m|n$ 时, $\varphi(m)|\varphi(n)$ 。

证明

$$\varphi(m) = \prod \varphi(p_i^{\alpha_i})$$

$$\varphi(n) = \prod \varphi(p_i^{\beta_i})$$

2.3 欧拉定理

2.3.1 欧拉定理和费马定理

定理 2.10 (欧拉定理)

设 m 为正整数, $(a, m) = 1$, 那么 $a^{\varphi(m)} \equiv 1 \pmod{m}$ 。



证明

设 $r_1, r_2, \dots, r_{\varphi(m)}$ 是模 m 的一个简化剩余系, 因为 $(a, m) = 1$, 由定理 2.4 可得, $ar_1, ar_2, \dots, ar_{\varphi(m)}$ 也是模 m 的简化剩余系, 因此对于任意 $1 \leq i \leq \varphi(m)$, 有且仅有唯一的 $1 \leq j \leq \varphi(m)$ 使得 $ar_j \equiv r_i \pmod{m}$, 所以

$$r_1 r_2 \cdots r_{\varphi(m)} \equiv ar_1 ar_2 \cdots ar_{\varphi(m)} \equiv a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}$$

由定理 2.4, $a^{\varphi(m)} \equiv 1 \pmod{m}$

定理 2.11 (费马小定理)

设 p 为素数, 那么对于任意整数 a , $a^p \equiv a \pmod{p}$ 。



证明

(1) 若 $(a, p) = 1$, 由欧拉定理, $a^{p-1} \equiv 1 \pmod{p}$ 。

(2) 若 $(a, p) \neq 1$, 那么 $p|a$, 所以 $a \equiv 0 \pmod{p}$, 此时仍有 $a^p \equiv a \equiv 0 \pmod{p}$ 。

欧拉定理和费马小定理反映了整数的幂关于模 m 的周期性。

练习 2.3 假设今天是星期三, 求 $2^{20170226}$ 天后是星期几。

解

因为 $\varphi(7) = 6$, 根据欧拉定理, $(2, 7) = 1$, $2^6 \equiv 1 \pmod{7}$, 所以, 对于任意整数 $k \geq 0$, $2^{6k} \equiv 1 \pmod{7}$ 。

又因为 $20170226 \equiv 2 \pmod{6}$, 此时 $2^{20170226} = 2^{6k+2} = 2^{6k} 2^2 \equiv 4 \pmod{7}$, 故此 $2^{20170226}$ 天后是星期天。

2.3.2 扩展欧拉定理

定理 2.12 (扩展的欧拉定理)

设 m 为正整数, 且 $m = \prod_{i=1}^s p_i^{a_i} (a_i > 0)$, a 为任意整数, 在 m 的素因子中, 仅当 $1 \leq i \leq s'$ 时, $p_i | a$, 那么, 对于任意 $k \geq 0$, $t \geq \max_{1 \leq i \leq s'} \{a_i\}$, 均有 $a^{k\varphi(m)+t} \equiv a^t \pmod{m}$ 。



结论 设 p_i 为素数, a 为任意整数, 那么, 对于任意 $k \geq 0$, $t \leq \beta_i$, 均有 $a^{k\varphi(\prod p_i^{\beta_i})+t} \equiv a^t \pmod{\prod p_i^{\beta_i}}$ 。

练习 2.4 $35^{20191443} \pmod{75}$

解

$$35^{k\varphi(75)+t} \equiv 35^t \pmod{3 \times 5^2}$$

因为 $\varphi(75) = \varphi(3)\varphi(25) = 2 \times 5 \times 4 = 40$

$$20191443 \equiv 3 \pmod{40}$$

所以可以得到 $t = 3$, 检验可知 $3 > 2, 3 > 1$

$$(5^2 \times 7)^{k\varphi(m)+1} \equiv (5^2 \times 7) \pmod{3 \times 5^2}$$

2.3.3 模重复平方算法

设 $e = (e_{n-1}e_{n-2}\cdots e_1e_0)_2$ 是 e 的二进制表示, 其中 $e_i (0 \leq i \leq n-1)$ 为 0 或 1, 那么:

$$\begin{aligned} a^e &= a^{e_{n-1}2^{n-1}+e_{n-2}2^{n-2}+\cdots+e_12+e_0} \\ &= (a^{2^{n-1}})^{e_{n-1}}(a^{2^{n-2}})^{e_{n-2}}\cdots(a^2)^{e_1}a^{e_0} \end{aligned}$$

若我们以此计算

$$\begin{aligned} b_0 &\equiv a \equiv a^{2^0} \pmod{m} \\ b_1 &\equiv b_0^2 \equiv a^{2^1} \pmod{m} \\ b_2 &\equiv b_1^2 \equiv a^{2^2} \pmod{m} \\ &\vdots \\ b_{n-1} &\equiv b_{n-2}^2 \equiv a^{2^{n-1}} \pmod{m} \end{aligned}$$

则 $a^e \equiv \prod_{e_i=1} b_i \pmod{m}$ 。

例题 2.5 试求 $2^{20170226} \pmod{84375}$

解

首先我们可以用欧拉定理化简, 因为 $84375 = 3^3 5^5$, 所以,


$$\varphi(84375) = 3^3 5^5 \times (1 - \frac{1}{3})(1 - \frac{1}{5}) = 4500$$

又因为 $2^{20170226} \equiv 2^{20170226 \pmod{4500}} \equiv 2^{10226} \pmod{84375}$, $10226 = (100111111110010)_2$,

计算 $b_0 \equiv 2, b_1 \equiv 4, b_2 \equiv 16, \cdots, b_n \equiv b_{n-1}^2, \cdots, b_{13} \equiv 74146 \pmod{84375}$

在计算过程中可以先和 84375 模的, 就尽可能模, 所以 $b_i < 84375$ 。

$$\begin{aligned} 2^{10226} &\equiv b_1 b_2 \cdots b_{13} \\ &\equiv 9019 b_5 b_6 b_7 b_8 b_9 b_{10} b_{13} \\ &\equiv 76999 b_6 \cdots \\ &\equiv 17884 b_7 \cdots \\ &\equiv 10354 b_8 \cdots \\ &\vdots \\ &\equiv 65614 \pmod{84375} \end{aligned}$$

 **笔记** $a^p \equiv a^{p \pmod{\varphi(m)}} \pmod{m}$

2.4 一次同余式

2.4.1 同余式及其解数

定义 2.4 (同余式及其解数)

设 $f(x) = \sum_{i=0}^n a_i x^i = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ 是一个整系数多项式, 为正整数, 那么称 $f(x) \equiv 0 \pmod{m}$ 为模 m 同余式。如果 $a_n \not\equiv 0 \pmod{m}$, 则称该同余式的次数为 n 。如果整数 a 满足 $f(a) \equiv 0 \pmod{m}$, 称 a 为同余式的解。

由定理 2.4 之 (5), 若 $b \equiv a \pmod{m}$, 则 $f(x) \equiv f(a) \equiv 0 \pmod{m}$, 所以 b 也是同余式的解, 一般地, 若 a 是同余式的解, 那么模 m 剩余类 \bar{a} 中的所有整数都是同余式的解, 记作 $x \equiv a \pmod{m}$ 。模 m 的完全剩

余系中同余式的解的个数称为同余式的解数。



例如, 3 满足同余式 $x^2 + 1 \equiv 0 \pmod{10}$, 所以剩余类 $x \equiv 3 \pmod{10}$ 中的整数都是同余式的解, 同样 $x \equiv 7 \pmod{10}$ 也是同余式的解, 该同余式的解数为 2。

2.4.2 一次同余式

定理 2.13

设 m 为正整数, 同余式 $ax \equiv b \pmod{m}$ 有解的充要条件是 $(a, m) | b$ 。在有解的情况下, 解数为 (a, m) , 且若 $x = x_0$ 是同余式的一个特解, 那么同余式的所有解可以表示为 $x \equiv x_0 + \frac{m}{(a, m)}t \pmod{m}$, $t = 0, 1, 2, \dots, (a, m) - 1$ 。



证明

$ax \equiv b \pmod{m}$ 有解也就是存在整数 y 使得 $ax - b = my$ 有解的充要条件是 $(a, m) | b$, 所以同余式 $ax \equiv b \pmod{m}$ 有解地充要条件是 $(a, m) | b$ 。

由定理 1.8, 若 $x = x_0, y = y_0$ 是 $ax - b = my$ 的一个解, 那么 $ax - b = my$ 的所有解可以表示为,

$$\begin{cases} x = x_0 + \frac{m}{(a, m)}t \\ y = y_0 + \frac{a}{(a, m)}t \\ t \in \mathbb{Z} \end{cases}$$

我们将 $x = x_0 + \frac{m}{(a, m)}t$ 写成 (a, m) 个模 m 的同余类为:

$$\overline{x_0}, \overline{x_0 + \frac{m}{(a, m)}}, \overline{x_0 + 2 * \frac{m}{(a, m)}}, \dots, \overline{x_0 + ((a, m) - 1) * \frac{m}{(a, m)}}$$

或者说原同余式的解为 $x \equiv x_0 + \frac{m}{(a, m)}t \pmod{m}$, $t = 0, 1, 2, \dots, (a, m) - 1$, 解数为 (a, m) 。

例题 2.6 试求同余式 $6x \equiv 28 \pmod{32}$ 的解。

解

因为 $(6, 32) = 2 | 28$, 所以同余式有两个解。

- 原同余式可以等价于 $3x \equiv 14 \pmod{16}$ 。
- 先求同余式 $3x \equiv 1 \pmod{16}$ 的解, $x \equiv -5 \pmod{16}$ 。
- 由此 $3x \equiv 14 \pmod{16}$ 的解为 $x \equiv -5 \times 14 \equiv 10 \pmod{16}$, $x = 10$ 是原同余式的一个特解。
- 原同余式的所有解为 $x \equiv 10 + 16t \pmod{16}$, $t = 0, 1$ 。

2.4.3 逆元

定义 2.5

设 m 为正整数, $(a, m) = 1$, 同余式 $ax \equiv 1 \pmod{m}$ 的解称为 a 模 m 的逆元, 记作 $x \equiv a^{-1}$, 当 $n \geq 0$ 时, 我们用 $a^{-n} \pmod{m}$ 来表示 $a^n \pmod{m}$ 的逆元



例题 2.7 试求整数 17 模 13 的逆元。

解

17 模 13 的逆元即求同余式 $17x \equiv 1 \pmod{13}$ 的解。同余式可以等价地变形为 $4x \equiv 1 \pmod{13}$, 因为 $4 \times 10 - 13 \times 3 = 1$, 所以 $4x \equiv 1 \pmod{13}$ 的解为 $x \equiv 10 \pmod{13}$, 该剩余类的所有整数均为 17 模 13 的逆元。

定理 2.14

设 m 为正整数, $(a, m) = 1$, 那么 $a^{\varphi(m)-1}$ 是 a 模 m 的逆元。



证明

因为 $(a, m) = 1$, 根据欧拉定理, 可以得到,

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

即 $a \cdot a^{\varphi(m)-1} \equiv 1 \pmod{m}$

所以 $x \equiv a^{\varphi(m)-1}$ 是同余式 $ax \equiv 1 \pmod{m}$ 的解, 由定义可知, $a^{\varphi(m)-1}$ 是 a 模 m 的逆元。

如果已知 a 模 m 的逆元 $x \equiv a^{-1} \pmod{m}$, 那么同余方程 $ax \equiv b \pmod{m}$ 的解可以写成 $x \equiv a^{-1}b \pmod{m}$ 。

例题 2.8 试证明: $(a^n)^{-1} \equiv (a^{-1})^n \pmod{m}$ 。

证明

- 当 $n \geq 0$, $a^n(a^{-1})^n \equiv 1 \pmod{m}$, 根据定义即可得证。
- 当 $n < 0$, $(a^{-1})^n \equiv ((a^{-1})^{-n})^{-1} \equiv ((a^{-n})^{-1})^{-1} \equiv (a^n)^{-1} \pmod{m}$

定理 2.15 (Wilson 定理)

设 p 是素数, 那么 $(p-1)! \equiv -1 \pmod{p}$ 。

**证明**

证明逆定理

$$((p-1)!, p) = (-1, p) = 1$$

证明正定理

若 $p = 2$, 结论显然成立。

设 $p > 2$, 对于 $1 \leq a \leq p-1$, 因为 $(a, p) = 1$, 所以 a 存在逆元 a' , 由 $ax \equiv 1 \pmod{m}$ 的解数为 1, 满足 $1 \leq a' \leq p-1$ 的逆元是唯一的。在 $1, 2, \dots, p-1$ 中, 如果 $a \neq a'$, 我们将 a 和 a' 配对, 得到 $aa' \equiv 1 \pmod{m}$ 。如果 $a = a'$, 得到 $a^2 \equiv aa' \equiv 1 \pmod{p}$, 只有 $a = 1$ 和 $a = p-1$, 所以, $(p-1)! \equiv 1 \times (p-1) \equiv -1 \pmod{p}$ 。

结论 设 p 是奇素数, 那么 $(\frac{p-1}{2}!)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}$ 。

证明

根据 Wilson 定理

$$\begin{aligned} 1 \times 2 \times \dots \times \frac{p-1}{2} \times \frac{p+1}{2} \times \dots \times (p-1) &\equiv -1 \pmod{p} \\ (\frac{p-1}{2}!)^2 (-1)^{\frac{p-1}{2}} &\equiv -1 \pmod{p} \\ (\frac{p-1}{2}!)^2 &\equiv (-1)^{\frac{p+1}{2}} \pmod{p} \end{aligned}$$



笔记 $a \equiv b \pmod{m} \Rightarrow (a, m) = (b, m)$

2.5 中国剩余定理

2.5.1 中国剩余定理

定理 2.16 (CRT)

设 m_1, m_2, \dots, m_s 为两两互素的正整数, b_1, b_2, \dots, b_s 为任意整数, 那么同余式组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \dots \\ x \equiv b_s \pmod{m_s} \end{cases}$$

模 $M = m_1 m_2 \dots m_s$ 有唯一解 $x \equiv \sum_{i=1}^s b_i \cdot \frac{M}{m_i} \left(\frac{M}{m_i}\right)^{-1} \pmod{m_i} \pmod{M}$



关于中国剩余定理的理解, 可以参考刘铎老师的知乎: <https://zhuanlan.zhihu.com/p/44591114>

例题 2.9 求解同余式

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 1 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 5 \pmod{7} \end{cases}$$

解

$$x \equiv 1 \times 105 \times 1 + 1 \times 70 \times 1 + 3 \times 42 \times 3 + 5 \times 30 \times 4 \equiv 1153 \equiv 103 \pmod{210}$$

如果将上述 $105 \pmod{2}$ 的逆元 1 换成其他代表比如 3, 结果还正确, 因为 $105 \times (1 + 2t) = 105 \times 1 + Mt \equiv 105 \pmod{M}$

2.5.2 递推法**例题 2.10** 求解同余式

$$\begin{cases} x \equiv 1 \pmod{11} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \\ x \equiv 4 \pmod{7} \end{cases}$$

解

$$x \equiv 1 \pmod{11} \Rightarrow x - 1 \equiv 0 \pmod{11}$$

$$x \equiv 2 \pmod{3} \Rightarrow x - 1 \equiv 1 \pmod{3}$$

$$\text{结合上面两式: } x - 1 \equiv 1 \times 11 \times (-1) \equiv -11 \pmod{33}$$

$$\text{由此, } x + 10 \equiv 0 \pmod{33}$$

$$\text{再由 } x \equiv 3 \pmod{5} \Rightarrow x + 10 \equiv 13 \equiv 3 \pmod{5}$$

$$\text{结合上面两式: } x + 10 \equiv 3 \times 33 \times 2 \equiv 198 \equiv 33 \pmod{165}$$

$$\text{由此, } x - 23 \equiv 0 \pmod{165}$$

$$\text{再由 } x \equiv 4 \pmod{7} \Rightarrow x - 23 \equiv -19 \equiv 2 \pmod{7}$$

$$\text{结合上面的两式: } x - 23 \equiv 2 \times 165 \times 2 \equiv 660 \pmod{1155} \Rightarrow x \equiv 683 \pmod{1155}$$

结论 $\begin{cases} x \equiv 0 \pmod{a} \\ x \equiv y \pmod{b} \end{cases} \Rightarrow x \equiv y \cdot a \cdot (a^{-1}) \pmod{b} \pmod{ab}$

例题 2.11 试用递推法, 求韩信点兵的问题:

$$\begin{cases} x \equiv 2(\text{mod } 3) \\ x \equiv 3(\text{mod } 5) \\ x \equiv 2(\text{mod } 2) \end{cases}$$

2.5.3 应用

例题 2.12 计算 $17^{20200301}(\text{mod } 105)$

解

$$17^{20200301} \equiv (-1)^{20200301} \equiv -1 \equiv 2(\text{mod } 3)$$

$$17^{20200301} \equiv 2^{20200301}(\text{mod } 4) \equiv 2(\text{mod } 5)$$

$$17^{20200301} \equiv 3^{20200301}(\text{mod } 6) \equiv 3^{-1} \equiv 5(\text{mod } 7)$$

根据中国剩余定理, 第 1, 2 式合并:

$$17^{20200301} \equiv 2 \times 7 \times (-2) + 5 \times 15 \times 1 \equiv 75 - 28 \equiv 47(\text{mod } 105)$$

例题 2.13 已知 RSA 解密密匙 (d, p, q) , 解密密文 C 。

解 一般解法, $m \equiv C^d(\text{mod } pq)$ 中国剩余定理解法:

$$m_1 \equiv C^{d(\text{mod } p-1)}(\text{mod } p)$$

$$m_2 \equiv C^{d(\text{mod } q-a)}(\text{mod } q)$$

$$m \equiv m_1 pq^{-1}(\text{mod } q) + m_2 pq^{-1}(\text{mod } p)(\text{mod } pq)$$

2.6 同余式组解法

2.6.1 同余式组解数

定理 2.17

设 m_1, m_2, \dots, m_s 为两两互素的正整数, 若对于 $1 \leq i \leq s$, 同余式 $f_i(x) \equiv 0(\text{mod } m_i)$ 有 C_i 个解, 那么, 同余式组

$$\begin{cases} f_1(x) \equiv 0(\text{mod } m_1) \\ f_2(x) \equiv 0(\text{mod } m_2) \\ \dots \\ f_s(x) \equiv 0(\text{mod } m_s) \end{cases}$$

对于模 $M = m_1 m_2 \dots m_s$ 有 $C_1 C_2 \dots C_s$ 个解。



证明

- 构造所有解

设 $f_i(x) \equiv 0(\text{mod } m_i)$ 的 C_i 个解为 $x \equiv b_{i,1}, b_{i,2}, \dots, b_{i,C_i}(\text{mod } m_i)$, 将这些解进行组合得到形式为

$$x \equiv \sum_{i=1}^s b_i \cdot \frac{M}{m_i} \left(\frac{M}{m_i} \right)^{-1}(\text{mod } m_i)(\text{mod } M)$$

的解, 其中, b_i 遍历 $b_{i,1}, b_{i,2}, \dots, b_{i,C_i}$, 解的个数为 $C_1 C_2 \dots C_s$ 。

- 两两互不同余

下面我们证明这些解关于模 M 是两两互不同余的。

若 $x' \equiv \sum_{i=1}^s b'_i \cdot \frac{M}{m_i} \left(\frac{M}{m_i} \right)^{-1}(\text{mod } m_i)(\text{mod } M)$ 是其中的一个解, 且 $x' \equiv x(\text{mod } M)$, 根据定理 2.2,

$$\begin{cases} x \equiv x' \pmod{m_1} \\ x \equiv x' \pmod{m_2} \\ \dots \\ x \equiv x' \pmod{m_s} \end{cases}, \text{ 可以得到 } \begin{cases} b_1 \equiv b'_1 \pmod{m_1} \\ b_2 \equiv b'_2 \pmod{m_2} \\ \dots \\ b_s \equiv b'_s \pmod{m_s} \end{cases}$$
 说明, 只要 b_i 中的任意一个发生变化, 得到的解都是不同的。

2.6.2 模同一素数幂

定理 2.18

设 p 为素数, $i_1 \geq i_2 \geq \dots \geq i_s$, b_1, b_2, \dots, b_s 为任意整数, 那么同余式组

$$\begin{cases} x \equiv b_1 \pmod{p^{i_1}} \\ x \equiv b_2 \pmod{p^{i_2}} \\ \dots \\ x \equiv b_s \pmod{p^{i_s}} \end{cases}$$

有解的充要条件是

$$\begin{cases} b_1 \equiv b_2 \pmod{p^{i_2}} \\ b_1 \equiv b_3 \pmod{p^{i_3}} \\ \dots \\ b_1 \equiv b_s \pmod{p^{i_s}} \end{cases}$$

如果有解, 其解为 $x \equiv b_1 \pmod{p^{i_1}}$ 。



例题 2.14 试判断同余式组 $\begin{cases} x \equiv 9 \pmod{15} \\ x \equiv 49 \pmod{50} \\ x \equiv -41 \pmod{140} \end{cases}$ 是否有解, 如果有解, 求出其解。

解

原同余式可以等价变形为 $\begin{cases} x \equiv 9 \pmod{3} \\ x \equiv 9 \pmod{5} \\ x \equiv 49 \pmod{5^2} \\ x \equiv 49 \pmod{2} \\ x \equiv -41 \pmod{7} \\ x \equiv -41 \pmod{2^2} \\ x \equiv -41 \pmod{5} \end{cases}$

$49 \equiv 9 \equiv -41 \pmod{5}$, $-41 \equiv 49 \pmod{2}$ 有解

可以等价地变形为

$$\begin{cases} x \equiv 9 \pmod{3} \\ x \equiv 49 \pmod{5^2} \\ x \equiv -41 \pmod{7} \\ x \equiv -41 \pmod{2^2} \end{cases}, \text{ 进一步化简为 } \begin{cases} x \equiv 0 \pmod{3} \\ x \equiv -1 \pmod{5^2} \\ x \equiv 1 \pmod{7} \\ x \equiv 3 \pmod{2^2} \end{cases}$$
 最后求得 $x \equiv 99 \pmod{2100}$ (用 CRT)。

2.6.3 一般同余式求解

对于合数 $m = \prod_{i=1}^s p_i^{\alpha_i}$, 求同余式 $f(x) \equiv 0 \pmod{m}$ 的解等价于求同余式组

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x) \equiv 0 \pmod{p_2^{\alpha_2}} \\ \dots \\ f(x) \equiv 0 \pmod{p_s^{\alpha_s}} \end{cases}$$

的解。

练习 2.5

- 试证明同余式组 $\begin{cases} x \equiv a \pmod{m} \\ x \equiv b \pmod{n} \end{cases}$ 有解的充要条件是 $(m, n) \mid a - b$
- 求解同余式组 $\begin{cases} x^2 \equiv 1 \pmod{7} \\ 4x \equiv 4 \pmod{6} \\ x \equiv 4 \pmod{9} \end{cases}$

2.7 模为素数幂的高层同余式

定义 2.6

设 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ 是一个正系数多项式, 其一阶导式 $f'(x) = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + a_1$. $f(x)$ 的一阶导式也可以记为 $f^{(1)}(x)$, 依次地, 定义其 m 阶导式为 $f^{(m)}(x) = (f^{(m-1)}(x))'$.

定理 2.19 (构造所有解)

设 p 为素数, $k \geq 1$, 那么 $x \equiv x_k \pmod{p^k}$ 是同余式 $f(x) \equiv 0 \pmod{p^k}$ 的一个解, 那么在这个剩余类中,

- 若 $(p, f'(x_k)) = 1$, 同余式 $f(x) \equiv 0 \pmod{p^{k+1}}$ 有唯一解。
- 若 $p \mid f'(x_k)$, 当 $f(x_k) \not\equiv 0 \pmod{p^{k+1}}$ 时, 同余式 $f(x) \equiv 0 \pmod{p^{k+1}}$ 无解; 当 $f(x_k) \equiv 0 \pmod{p^{k+1}}$ 时, 同余式 $f(x) \equiv 0 \pmod{p^{k+1}}$ 有 p 个解

证明

- 根据定理 2.2, 同余式 $f(x) \equiv 0 \pmod{p^{k+1}}$ 的解一定满足 $f(x) \equiv 0 \pmod{p^k}$ 所以 $f(x) \equiv 0 \pmod{p^{k+1}}$ 的解可以从 $f(x) \equiv 0 \pmod{p^k}$ 的解中进行筛选而得。
- 因为 $x \equiv x_k \pmod{p^k}$ 是同余式 $f(x) \equiv 0 \pmod{p^k}$ 的一个解, 我们将从

$$x = x_k + p^k t, t \in \mathbb{Z}$$

这个剩余类中筛选出 $f(x) \equiv 0 \pmod{p^{k+1}}$ 的解。

将 $x = x_k + p^k t$ 代入 $f(x) \equiv 0 \pmod{p^{k+1}}$, 有 $f(x_k + p^k t) \equiv 0 \pmod{p^{k+1}}$, 用泰勒公式展开得到

$$f(x_k) + f'(x_k) p^k t + \sum_{i=2}^n \frac{f^{(i)}(x_k) p^{ik}}{i!} t^i \equiv 0 \pmod{p^{k+1}}$$

进一步化简可得

$$f(x_k) + f'(x_k) p^k t \equiv 0 \pmod{p^{k+1}}$$

由 $f(x_k) \equiv 0 \pmod{p^k}$, 有 $p^k \mid f(x_k)$, 所以上式可以进一步化简为

$$f'(x_k) t \equiv -\frac{f(x_k)}{p^k} \pmod{p}$$

(1) 若 $(f'(x_k), p) = 1$, 上式有唯一解 $t \equiv -\frac{f(x_k)}{p^k}(f'(x_k))^{-1}(\text{mod } p)$, 从而筛得 $f(x) \equiv 0(\text{mod } p^{k+1})$ 的解为

$$\begin{aligned} x &\equiv x_0 - \frac{f(x_k)}{p^k}((f'(x_k))^{-1}(\text{mod } p))p^k \\ &\equiv x_k - f(x_k)((f')^{-1}(\text{mod } p))(\text{mod } p^{k+1}) \end{aligned}$$

(2) 若 $p \mid f'(x_k)$, 当 $f(x_k) \not\equiv 0(\text{mod } p^{k+1})$ 时, 上式无解;

当 $f(x_k) \equiv 0(\text{mod } p^{k+1})$ 时, 上式有 p 个解, 也就是说 $x = x_k + p^k t, t \in \mathbb{Z}, x \equiv x_k + p^k t(\text{mod } p^{k+1}), t = 0, 1, \dots, p-1$ 。

结论 设 p 为素数, 若 $x \equiv x_1(\text{mod } p)$ 是同余式 $f(x) \equiv 0(\text{mod } p)$ 的一个解, 且满足 $(f'(x_1), p) = 1$, 那么对于任意正整数 $k > 1$, $f(x) \equiv 0(\text{mod } p^k)$ 的满足 $x \equiv x_1(\text{mod } p)$ 的解 x_k 可以通过如下递推公式得到:

$$x_i \equiv x_{i-1} - f(x_{i-1})((f')^{-1}(\text{mod } p))(\text{mod } p^i), \quad i = 2, 3, \dots, k$$

证明

利用数学归纳法可以证明。

2.8 高次同余式求解方法

2.8.1 唯一解

例题 2.15 试求同余式 $x^3 + 4x^2 + 1 \equiv 0(\text{mod } 3^5)$ 的解

解

令 $f(x) = x^3 + 4x^2 + 1$, 则 $f'(x) = 3x^2 + 8x \equiv 2x(\text{mod } 3)$

由同余式 $f(x) \equiv 0(\text{mod } 3)$ 得到解 $x_1 \equiv 1(\text{mod } 3)$

所以, $(f'(x_1))^{-1} \equiv 2^{-1} \equiv 2(\text{mod } 3)$

根据定理的推论有

$$\begin{aligned} x_2 &\equiv x_1 - 2f(x_1) \equiv 7(\text{mod } 3^2) \\ x_3 &\equiv x_2 - 2f(x_2) \equiv 7(\text{mod } 3^3) \\ x_4 &\equiv x_3 - 2f(x_3) \equiv 61(\text{mod } 3^4) \\ x_5 &\equiv x_4 - 2f(x_4) \equiv 142(\text{mod } 3^5) \end{aligned}$$

所以, 原同余式的解为 $x \equiv 142(\text{mod } 3^5)$

2.8.2 无解

例题 2.16 试求同余式 $x^2 + p \equiv 0(\text{mod } p^3)$, 其中 p 为奇素数。

解

令 $f(x) = x^2 + p$, 则 $f'(x) \equiv 2x(\text{mod } p)$

考虑 $f(x) \equiv 0(\text{mod } p)$, 它的唯一解为 $x_1 \equiv 0(\text{mod } p)$

$f'(x_1) \equiv 0(\text{mod } p)$, 所以 $p \mid f'(x_1)$

因为 $f(x_1) = p$, 所以 $p^2 \nmid f(x_1)$, 根据定理, 同余式 $x^2 + p \equiv 0(\text{mod } p^2)$ 无解, 原同余式也一定无解。

2.8.3 多个解

例题 2.17 试求解同余式 $x^2 - p^2 \equiv 0(\text{mod } p^3)$, 其中 p 为奇素数。

解

令 $f(x) = x^2 - p^2$, 则 $f'(x) \equiv 2x(\text{mod } p)$

考虑 $f(x) \equiv 0 \pmod{p}$, 它有唯一解 $x_1 \equiv 0 \pmod{p}$

$f'(x_1) \pmod{p}$, 所以 $p \nmid f'(x_1)$

$f(x_1) = -p^2$, 所以 $p^2 \mid f(x_1)$, 根据定理, 同余式 $x^2 - p^2 \equiv 0 \pmod{p^2}$ 有 p 个解, $x_2 = 0, p, 2p, \dots, (p-1)p \pmod{p^2}$

$f(x_2) = (ip)^2 - p^2 = (i^2 - 1)p^2$, 仅当 $i = 1, -1$ 时, $p^3 \mid f(x_2)$, 所以, 同余式 $x^2 - p^2 \equiv 0 \pmod{p^3}$ 的解为:

$x_3 \equiv \pm p, p^2 \pm p, 2p^2 \pm p, \dots, (p-1)p^2 \pm p \pmod{p^3}$

2.8.4 复杂情况

- 转化为素数幂 (简化模)

对于合数 $m = \prod_{i=1}^s p_i^{\alpha_i}$, 求同余式 $f(x) \equiv 0 \pmod{m}$ 的解等价于求同余式组

$$\begin{cases} f(x) \equiv 0 \pmod{p_1^{\alpha_1}} \\ f(x) \equiv 0 \pmod{p_2^{\alpha_2}} \\ \dots \\ f(x) \equiv 0 \pmod{p_s^{\alpha_s}} \end{cases}$$

的解

- 扩展欧拉定理之结论 (降次)

设 p 为素数, a 为任意整数, 那么, 对于任意 $k \geq 0, t \geq \beta$, 均有 $a^{k\varphi(p^\beta)+t} \equiv a^t \pmod{p^\beta}$ 。

例题 2.18 求解同余式 $x^{254} + 2x^3 \equiv 0 \pmod{135}$

解

$$\begin{cases} x^2 + 2x^3 \equiv 0 \pmod{5} \Leftrightarrow x^2(1+2x) \equiv 0 \pmod{5} \Rightarrow x \equiv 0, 2 \pmod{5} \\ x^{254} + 2x^3 \equiv 0 \pmod{27} \Leftrightarrow x^{20} + 2x^3 \equiv 0 \pmod{27} \end{cases}$$

令 $f(x) = x^{20} + 2x^3$, 则 $f(x) \equiv 0 \pmod{3}$ 得解 $x_1 \equiv 0, 1 \pmod{3}$

$f'(x) \equiv 2x \pmod{3}$, $f'(1) \equiv 2 \pmod{3}$, $f'(1)^{-1} \equiv 2 \pmod{3}$, 由 $x_1 \equiv 1 \pmod{3}$, 所以

$x_2 \equiv 1 - 2 * f(1) \pmod{9} \equiv 4 \pmod{9}$

$x_3 \equiv 4 - 3 * f(4) \pmod{27} \equiv 4 - 2(4^2 + 2 * 4^3) \equiv 13 \pmod{27}$

由 $x_1 \equiv 0 \pmod{3}$, 由于 $3t + x_1$ 均满足 $x^{254} + 2x^3 \equiv 0 \pmod{27}$, 所以 $x_3 \equiv 0, 3, 6, 9, \dots, 24 \pmod{27}$

综上所述得到

$$\begin{cases} x \equiv a \equiv 0 \pmod{5} \\ x \equiv b \equiv 0, 3, 6, 9, 12, 13, 15, 18, 21, 24 \pmod{27} \end{cases}$$

综上所述, 根据中国剩余定理, 所有解为:

$x \equiv a \cdot 27 \cdot ((27)^{-1} \pmod{5}) + b \cdot 5 \cdot 11 \pmod{135}$

$x \equiv 0, 30, 60, 90, 120, 40, 15, 45, 75, \dots$

第2章 练习

1. 试证明: 如果 $r_1, r_2, \dots, r_{\varphi(m)}$ 是模 $m(m > 2)$ 的一个简化剩余系, 那么 $\sum_{i=1}^{\varphi(m)} r_i \equiv 0 \pmod{m}$ 。
2. 试证明: 如果 n 是正奇数, 那么 $\sum_{i=1}^{n-1} i^3 \equiv 0 \pmod{n}$ 。
3. 试判断 128749832749837759345 是否是 11 和 13 的倍数。
4. 试计算 $13^{20170226} \pmod{72}$ 。
5. 试证明: 若 $N = \prod_{i=1}^n p_i^{\alpha_i}$, $(a, N) = 1$, 那么

$$a^{[\varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}), \dots, \varphi(p_n^{\alpha_n})]} \equiv 1 \pmod{N}$$

6. 试证明：正整数 $N > 1$ 满足 $\varphi(N) = 2^n$ 的充要条件是 N 有分解式 $N = 2^m \prod_{i=1}^S F_i$, $m \geq 0$, F_i 为互不相等的 Fermat 素数。
7. RSA 加密算法。设 $N = pq$, p, q 为不相等的素数, 正整数 e 满足 $(e, \varphi(N)) = 1$, d 满足 $ed \equiv 1 \pmod{\varphi(N)}$, 试证明：对于任意明文 $0 \leq m < N$, 若加密算法为 $c \equiv m^e \pmod{N}$, 那么由密文 c , 可以通过计算 $c^d \pmod{N}$ 解密得到明文 m 。
8. 试证明：正整数 $N > 1$ 对于任意整数 $0 \leq a < N$ 和 $k > 0$ 均有 $a^{k\varphi(N)+1} \equiv a \pmod{N}$ 的充要条件是 N 有分解式 $N = \prod_{i=1}^n p_i$, p_i 为互不相等的素数。
9. 设模 m 的简化剩余系为 $r_1, r_2, \dots, r_{\varphi(m)}$, 试证明： $(\prod_{i=1}^{\varphi(m)} r_i)^2 \equiv 1 \pmod{m}$ 。
10. 试求解一次同余式 $256x \equiv 28 \pmod{400}$ 。
11. 如果 p 是素数, 且 $p \equiv 1 \pmod{4}$, 那么同余式 $x^2 \equiv -1 \pmod{p}$ 有两个不同余的解

$$x \equiv \pm \frac{p-1}{2}! \pmod{p}$$
12. 试计算 $3^{20100416} \pmod{35}$, $3^{20150410} \pmod{35 \times 27}$ 。
13. 试证明：如果 $(a, 32760) = 1$, 那么 $a^{12} \equiv 1 \pmod{32760}$ 。
14. 求解同余式 $x^{10} + x^2 + x + 1 \equiv 0 \pmod{2^5}$ 。
15. 求解同余式 $x^2 + px \equiv 0 \pmod{p^3}$, 其中 p 为奇素数。

第3章 域

3.1 域的定义与性质

3.1.1 域的定义

定义 3.1

设 \mathbb{F} 是一个非空集合，对其上定义了两种运算，分别叫做加法和乘法，记作 “+”, “ \cdot ”，对于 \mathbb{F} 中的任意两个元素 a, b ，均有 $a + b \in \mathbb{F}$, $a \cdot b \in \mathbb{F}$ (\mathbb{F} 对于加法和乘法自封闭)， $a + b$, $a \cdot b$ 分别称为两个元素的和与积， $a \cdot b$ 通常记作 ab)，我们称 \mathbb{F} 对于所规定的加法和乘法成为一个域，如果其元素满足以下运算规则：

- \mathbb{F} 中所有元素对于加法形成一个加法交换群；
- \mathbb{F} 中所有非零元素 (\mathbb{F}^*) 对于乘法形成一个乘法交换群；
- 对于任意 $a, b, c \in \mathbb{F}$, $a(b + c) = ab + ac$ (乘法对加法的分配律).



一个域至少有两个元素，即**加法群的零元**和**乘法群的单位元**，他们分别称为域的零元和单位元，记作 0 和 1 ，单位元有时也记作 e 。当称一个集合是域的时候，除了需要指明集合本身的元素外，还要指明集合上定义的加法和乘法。

当域的元素个数有限时称为**有限域**，或者**伽罗华域**，否则称为**无限域**。常见的有理数集合 \mathbb{Q} ，实数集合 \mathbb{R} 和复数集合 \mathbb{C} 按照其上定义的加法和乘法都形成域，分别叫做有理数域，实数域和复数域。

例题 3.1 以下集合按照定义的加法和乘法均不形成域：

- (1) 全体整数形成的集合 \mathbb{Z} ，加法和乘法分别为 \mathbb{Z} 上的加法和乘法；
- (2) 集合 $\{a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\}$ ，加法和乘法分别为实数域 \mathbb{R} 上的加法和乘法；
但是 $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ 是一个域；
- (3) $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$ ， m 为合数，加法和乘法分别为模 m 的加法和乘法。

定理 3.1

设 \mathbb{F} 是一个域，那么

- (1) 对于任意 $a \in \mathbb{F}$, $0a = a0 = 0$ 。
- (2) 任意 $a, b \in \mathbb{F}$, if $ab = 0$, $\Rightarrow a = 0$ or $b = 0$ 。



3.1.2 子域和扩域

定义 3.2

设 \mathbb{F} 是一个域， \mathbb{F}_0 是 \mathbb{F} 的非空子集，如果对于 \mathbb{F} 上的加法和乘法， \mathbb{F}_0 也是一个域，则称 \mathbb{F}_0 是 \mathbb{F} 的子域， \mathbb{F} 是 \mathbb{F}_0 的扩域，记作 $\mathbb{F}_0 \subset \mathbb{F}$ 。



例如： $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{R} \subset \mathbb{R}[\sqrt{-2}] \subset \mathbb{C}$ 。

判断方法

定理 3.2

设 $\mathbb{F}_0, \mathbb{F}_0^*$ 均是域 \mathbb{F} 的非空子集, 当且仅当以下条件成立时 \mathbb{F}_0 是域 \mathbb{F} 的子域:

- (1) 任意 $a, b \in \mathbb{F}_0$, 都有 $-a, a+b \in \mathbb{F}_0$;
- (2) 任意非零元素 $a, b \in \mathbb{F}_0$, 都有 $a^{-1}, ab \in \mathbb{F}_0$.



证明

- (1) 说明 \mathbb{F}_0 是 \mathbb{F} 的加法子群
- (2) 说明 \mathbb{F}_0^* 是 \mathbb{F}^* 的乘法子群。

而乘法对加法的分配律在 \mathbb{F} 中成立, 那么在 \mathbb{F}_0 中也必然成立, 根据定义 \mathbb{F}_0 是一个域。

例题 3.2

- (1) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, 加法和乘法分别为实数域 \mathbb{R} 上的加法和乘法;
- (2) $\mathbb{Z}_p = \{0, 1, \dots, p-1\}$, p 为素数, 加法和乘法分别为模 p 的加法和乘法;

3.2 域的特征

3.2.1 特征的定义

定义 3.3

设 \mathbb{F} 是一个域, 如果存在正整数 m , 使得对于任意 $a \in \mathbb{F}$ 均有 $ma = 0$, 则在所有 m 中, 最小的正整数称为域 \mathbb{F} 的**特征**; 否则, 如果不存在正整数 m , 使得对于任意 $a \in \mathbb{F}$ 均有 $ma = 0$, 则称域 \mathbb{F} 的**特征为 0**。域 \mathbb{F} 的特征记作 $\text{char}(\mathbb{F})$ 。



3.2.2 域的同构

定义 3.4

设 \mathbb{F}, \mathbb{K} 是两个域, 如果存在 \mathbb{F} 到 \mathbb{K} 上的一一映射 δ , 使得对于任意 $a, b \in \mathbb{F}$, 均有

$$\delta(a+b) = \delta(a) + \delta(b), \delta(ab) = \delta(a)\delta(b)$$

则称 δ 为 \mathbb{F} 到 \mathbb{K} 上的**同构映射**, 此时称域 \mathbb{F}, \mathbb{K} 同构, 记作 $\mathbb{F} \cong \mathbb{K}$ 。如果 $\mathbb{F} = \mathbb{K}$, 则称 δ 为**自同构映射**, 特别地, 若进一步对于任意 $a \in \mathbb{F}$ 均有 $\delta(a) = a$, 则称 δ 为**恒等自同构映射**。



3.2.3 素域

一个域的最小子域称为该域的**素域**

定理 3.3


设 \mathbb{F} 是一个域, 如果 $\text{char}(\mathbb{F})$ 为正整数, 则必为某个素数 p 。特征为素数 p 的域的素域与 \mathbb{Z}_p 同构, 特征为 0 的域的素域与 \mathbb{Q} 同构。



证明 反证法。假设 $\text{char}(\mathbb{F}) = m > 0$, m 为合数。设 p 是 m 的最小素因子, $m = ps$, $1 < p < m$, $1 < s < m$, 则 $(ps)e = me = 0$, 而 $(ps)e = (pe)(se)$, 根据定理 3.1, $pe = 0$ 或者 $se = 0$ 。但是对于任意 $a \in \mathbb{F}$, $pa = (pe)a$, $sa = (se)a$, 所以必有 $pa = 0$ 或者 $sa = 0$, 这与 m 的最小性相矛盾。

当 $\text{char}(\mathbb{F}) = p$ 时, 可以验证 $\mathbb{F}_0 = \{0, e, 2e, \dots, (p-1)e\}$ 是域 \mathbb{F} 的最小子域, 而映射 $\delta: \mathbb{F}_0 \rightarrow \mathbb{Z}_p$, $\delta(ie) = i$ 为域同构映射。

当 $\text{char}(\mathbb{F}) = 0$ 时, 可以验证 $\mathbb{F}_0 = \{(ae)(be)^{-1} \mid a, b \in \mathbb{Z}, b \neq 0\}$ 是域 \mathbb{F} 的最小子域, 而映射 $\delta: \mathbb{F}_0 \rightarrow \mathbb{Q}, \delta((ae)(be)^{-1}) = \frac{a}{b} \in \mathbb{Z}, b \neq 0$ 为域同构映射。

 **练习 3.1** 试证明对于任何非负整数 n , 在特征为 p 的有限域 \mathbb{F} 上定义的映射 $\delta_n: \mathbb{F} \rightarrow \mathbb{F}, \delta_n(\alpha) = \alpha^{p^n}$ 均是 \mathbb{F} 的自同构。

3.3 二项式定理

3.3.1 二项式定理

定理 3.4 (二项式定理)

设 \mathbb{F} 是一个域, $a, b \in \mathbb{F}$, 则对于任意正整数 n , $(a+b)^n = \sum_{i=0}^n \binom{n}{i} a^{n-i} b^i$



3.3.2 特征幂的二项式定理

定理 3.5

设 \mathbb{F} 是一个域, $\text{char}(\mathbb{F}) = p$, 则对于任意 $a, b \in \mathbb{F}, n \geq 0$, 均有

$$(a \pm b)^{p^n} = a^{p^n} \pm b^{p^n}$$



证明 $n=0$ 时结论成立。

下面对 $n > 0$ 使用数学归纳法证明 $(a+b)^{p^n} = a^{p^n} + b^{p^n}$ 。

$n=1$ 时, 因为 $p \mid \binom{p}{i} (0 < i < p)$, 根据二项式定理, $(a+b)^p = a^p + b^p$ 。

假设 $n=k$ 时结论成立, 当 $n=k+1$ 时,

$$\begin{aligned} (a+b)^{p^{k+1}} &= ((a+b)^{p^k})^p = (a^{p^k} + b^{p^k})^p = a^{p^{k+1}} + b^{p^{k+1}}, \\ (a-b)^{p^n} &= (a+(-b))^{p^n} = a^{p^n} + (-1)^{p^n} b^{p^n}, \end{aligned}$$

当 $p \neq 2$ 时, $(-1)^{p^n} = -1$, 所以, $(a-b)^{p^n} = a^{p^n} - b^{p^n}$;

当 $p=2$ 时, $(-1)^{p^n} = 1 = -1$, 仍有 $(a-b)^{p^n} = a^{p^n} - b^{p^n}$ 。

3.3.3 域上的多项式

定义 3.5

对于非负整数 $i, a_i x^i, a_i \in \mathbb{F}$ 表示域 \mathbb{F} 上文字为 x 的**单项式**, 我们称形式和 $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x^1 + a_0 x^0, a_i \in \mathbb{F}$ 为域 \mathbb{F} 上的文字为 x 的**多项式**, 简称为域 \mathbb{F} 上的多项式。



3.3.4 多项式的加法和乘法

在 \mathbb{F} 上可以定义加法“+”和乘法“·”, 设 $f(x) = \sum_{i=0}^n a_i x^i, g(x) = \sum_{i=0}^m b_i x^i, n \geq m, b_{m+1} = b_{m+2} = \cdots = b_n = 0$, 则可定义

$$\begin{aligned} f(x) + g(x) &= \sum_{i=0}^n (a_i + b_i) x^i, \\ f(x) \cdot g(x) &= \sum_{j=0}^{m+n} \left(\sum_{i=0}^j a_i b_{j-i} \right) x^j \end{aligned}$$

关于多项式的次数, 下面结论成立:

$$\deg(f(x) + g(x)) \leq \max\{\deg f(x), \deg g(x)\}$$

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x)$$

$\mathbb{F}[x]$ 按照上面的定义加法和乘法 **不是域**, 因为除了 \mathbb{F} 中的非零元素, $\mathbb{F}[x]$ 中的其他元素均没有逆元。

$f(x), g(x)$ 是特征为 p 的域上的多项式, 那么

$$(f(x) \pm g(x))^{p^n} = f(x)^{p^n} \pm g(x)^{p^n}$$

$\mathbb{F}(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in \mathbb{F}[x], g(x) \neq 0 \right\}$ 按照以下运算规则形成一个域, 其中 $\frac{f(x)}{g(x)} + \frac{s(x)}{t(x)} = \frac{f(x)t(x) + s(x)g(x)}{g(x)t(x)}$, $\frac{f(x)}{g(x)} \frac{s(x)}{t(x)} = \frac{f(x)s(x)}{g(x)t(x)}$, 且 $\frac{f(x)}{g(x)} = \frac{f_1(x)}{g_1(x)}$ 当且仅当 $f(x)g_1(x) = g(x)f_1(x)$ 。特别地, 当 \mathbb{F} 是特征为 p 的有限域时, $\mathbb{F}(x)$ 是特征为 p 的无限域。

3.4 多项式的辗转相除法

3.4.1 带余除法算式

定理 3.6

设 $f(x), g(x)$ 为域 \mathbb{F} 上的两个多项式, $g(x) \neq 0$, 则存在唯一的一对多项式 $q(x), r(x)$, 使得:

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

$r(x)$ 称为 $f(x)$ 被 $g(x)$ 除所得的余式, 记作 $(f(x))_{g(x)} = r(x)$ 。



证明 设 $f(x) = a_n x^n + \cdots + a_1 x + a_0$, $g(x) = b_m x^m + \cdots + b_1 x + b_0$ 。

- **归纳基础** 当 $n < m$ 时, 取 $q(x) = 0$, $r(x) = f(x)$, 结论成立。
- **归纳假设** 假设当 $n < k (k \geq m)$ 时结论均成立。

定理 3.7

设 $f_1(x), f_2(x), g(x)$ 为域 \mathbb{F} 上的多项式, $g(x) \neq 0$, 则

$$(f_1(x) + f_2(x))_{g(x)} = (f_1(x))_{g(x)} + (f_2(x))_{g(x)}$$

$$(f_1(x)f_2(x))_{g(x)} = ((f_1(x))_{g(x)}(f_2(x))_{g(x)})_{g(x)}$$



证明

$$\begin{aligned} (f_1(x) + f_2(x))_{g(x)} &= (q_1(x)g(x) + (f_1(x))_{g(x)} + q_2(x)g(x) + (f_2(x))_{g(x)})_{g(x)} \\ &= ((q_1(x) + q_2(x))g(x) + (f_1(x))_{g(x)} + (f_2(x))_{g(x)})_{g(x)} \\ &= (f_1(x))_{g(x)} + (f_2(x))_{g(x)} \end{aligned}$$

$$\begin{aligned} (f_1(x)f_2(x))_{g(x)} &= ((q_1(x)q_2(x)g(x) + q_1(x)(f_2(x))_{g(x)} + q_2(x)(f_1(x))_{g(x)}g(x) + (f_1(x))_{g(x)}(f_2(x))_{g(x)})_{g(x)} \\ &= ((f_1(x))_{g(x)}(f_2(x))_{g(x)})_{g(x)} \end{aligned}$$

该定理可推广到多个多项式相加和相乘的情况。我们将以上运算分别叫做多项式 $f_1(x), f_2(x)$ 对 $g(x)$ 的模加和模乘运算。

3.4.2 因式与倍式

定义 3.6

设 $f(x)$ 为域 \mathbb{F} 上的多项式, 如果 $f(x)$ 的因式只有 $c, cf(x)$, 其中 $c \in \mathbb{F}^*$, 则 $f(x)$ 称为域 \mathbb{F} 上的不可约多项式, 否则称为可约多项式。



定理 3.8

域 \mathbb{F} 的多项式 $g(x) \mid f_1(x), g(x) \mid f_2(x)$, 那么对于 \mathbb{F} 上的任意多项式 $s(x), t(x)$

$$g(x) \mid s(x)f_1(x) + t(x)f_2(x)$$



例题 3.3 设 $f(x) = x^2 + 1$, 则 $f(x)$ 是实数域 \mathbb{R} 上的不可约多项式, 也是域 \mathbb{Z}_3 上的不可约多项式, 但 $f(x)$ 是复数域 \mathbb{C} 上的可约多项式, 在 \mathbb{C} 上 $f(x) = (x + \sqrt{-1})(x - \sqrt{-1})$, $f(x)$ 也是域 \mathbb{Z}_2 上的可约多项式, 在 \mathbb{Z} 上 $f(x) = (x + 1)^2$ 。

3.4.3 辗转相除法

定理 3.9

设 $r_0(x), r_1(x)$ 为域 \mathbb{F} 上的两个多项式, $r_1(x) \neq 0$, 则可以得如下带余除法算式:

$$r_0(x) = q_1(x)r_1(x) + r_2(x), \quad 0 \leq \deg r_2(x) < \deg r_1(x)$$

$$r_1(x) = q_2(x)r_2(x) + r_3(x), \quad 0 \leq \deg r_3(x) < \deg r_2(x)$$

... ..

$$r_{n-2}(x) = q_{n-1}(x)r_{n-1}(x) + r_n(x), \quad 0 \leq \deg r_n(x) < \deg r_{n-1}(x)$$

$$r_{n-1}(x) = q_n(x)r_n(x) + r_{n+1}(x), \quad r_{n+1}(x) = 0$$

- 经过若干步后, 余式必然为 0;
- 存在多项式 $s(x), t(x) \in \mathbb{F}[x]$, 使得 $s(x)r_0(x) + t(x)r_1(x) = r_n(x)$;
- 设 $r_n(x)$ 首项系数为 c , 则 $(r_0(x), r_1(x)) = c^{-1}r_n(x)$, 且最高公因式是唯一存在的。
- 对于任意 $d(x) \in \mathbb{F}[x]$, 若 $d(x) \mid r_0(x), d(x) \mid r_1(x)$, 那么 $d(x) \mid (r_0(x), r_1(x))$ 。



练习 3.2 在 \mathbb{Z}_3 中 $f(x) = x^3 + x^2 + x + 1, g(x) = 2x^4 + x^2$ 试求多项式 $s(x), t(x)$, 使得 $s(x)f(x) + t(x)g(x) = \gcd(f(x), g(x))$ 。

3.5 多项式整除和唯一因式分解定理

3.5.1 多项式整除的性质

定理 3.10

设 $f(x), g(x)$ 为域 \mathbb{F} 上两个不全为零的多项式, 则对于任意 $k(x) \in \mathbb{F}[x], (f(x) + g(x)k(x), g(x)) = (f(x), g(x))$ 。



定理 3.11

设 $p(x), f_1(x), f_2(x)$ 为域 \mathbb{F} 上的多项式, 且 $p(x) \mid f_1(x)f_2(x)$, 若 $(p(x), f_1(x)) = 1$, 则 $p(x) \mid f_2(x)$ 。



定理 3.12

设 $p(x)$, $f_1(x)$, $f_2(x)$ 为域 \mathbb{F} 上的多项式, $p(x)$ 为域 \mathbb{F} 上的不可约多项式, 且 $p(x) \mid f_1(x)f_2(x)$, 则 $p(x) \mid f_1(x)$ 或者 $p(x) \mid f_2(x)$ 。

**3.5.2 多项式的模逆**

结论 设 $f(x)$, $g(x)$ 为域 \mathbb{F} 上两个次数大于 0 的多项式, 那么, 存在唯一的一对多项式 $s(x)$, $t(x) \in \mathbb{F}[x]$, 使得 $s(x)f(x) + t(x)g(x)$, 且 $\deg s(x) < \deg g(x) - \deg(f(x), g(x))$, $\deg t(x) < \deg f(x) - \deg(f(x), g(x))$

证明

$$s(x)f(x) + t(x)g(x) = (f(x), g(x)) = d(x)$$

$$s(x)\frac{f(x)}{d(x)} + t(x)\frac{g(x)}{d(x)} = 1$$

$$\deg s(x) < \deg\left(\frac{g(x)}{d(x)}\right) = \deg g(x) - \deg d(x)$$

$$\deg t(x) < \deg\left(\frac{f(x)}{d(x)}\right) = \deg f(x) - \deg d(x)$$

证明 $u(x)f(x) + v(x)g(x) = 1 \Rightarrow \deg u(x) < \deg g(x)$.

$$u(x) = q_1(x)g(x) + s(x), \deg s(x) < \deg g(x),$$

$$v(x) = q_2(x)f(x) + t(x), \deg t(x) < \deg f(x),$$

得到:

$$(q_1(x)g(x) + s(x))f(x) + (q_2(x)f(x) + t(x))g(x) = 1$$

所以, $(q_1(x) + q_2(x))f(x)g(x) = 1 - (s(x)f(x) + t(x)g(x))$

两边次数做比较,

$$\deg((q_1(x) + q_2(x))f(x)g(x)) = \deg(q_1(x) + q_2(x)) + \deg(f(x)g(x))$$

$$\deg(1 - (s(x)f(x) + t(x)g(x))) < \deg((f(x)g(x)))$$

所以, $q_1(x) + q_2(x) = 0$, 于是

$$s(x)f(x) + t(x)g(x) = 1$$

所以得到 $\deg s(x) < \deg g(x) \Rightarrow \deg u(x) < \deg g(x)$ 。

3.5.3 唯一因式分解定理**定理 3.13**

设 $f(x)$ 是域 \mathbb{F} 上的次数大于 0 的多项式, 则 $f(x)$ 可以唯一地表示为域 \mathbb{F} 上一些次数大于 0 的不可约多项式的乘积。特别地, 设 $f(x)$ 是首 1 多项式, 且,

$$f(x) = p_1(x)p_2(x) \cdots p_s(x) = q_1(x)q_2(x) \cdots q_t(x)$$

其中 $p_1(x)$, $p_2(x)$, \cdots , $p_s(x)$, $q_1(x)$, $q_2(x)$, \cdots , $q_t(x)$ 均为域 \mathbb{F} 上次数大于 0 的首 1 不可约多项式, 则 $s = t$, 经过适当的调整可使 $p_1(x) = q_1(x)$, $p_2(x) = q_2(x)$, \cdots , $p_s(x) = q_s(x)$ 。



练习 3.3 $f(x)$ 是 n 次多项式, $f(x)$ 可约的充要条件是存在次数小于或者等于 $\lfloor \frac{n}{2} \rfloor$ 的首 1 不可约因式。试判断 $f(x) = x^7 + x + 1 \in \mathbb{Z}_2[x]$ 是否可约?

练习 3.4 试判断 $f(x) = x^7 + x + 1 \in \mathbb{Q}[x]$ 是否可约?

3.6 扩域的构造

- 任何有限域元素的个数为 p^n , $n \geq 1$, p 为素数
- 任意 p^n 的有限域都存在
- 元素个数相同的有限域是同构的

3.6.1 多项式的根

定义 3.7

设 $f(x)$ 为域 \mathbb{F} 上的多项式, 如果 $a \in \mathbb{F}$ 使得 $f(a) = 0$, 则称 a 为 $f(x)$ 在域 \mathbb{F} 中的一个根。



定理 3.14 (余元定理)

设 $f(x)$ 为域 \mathbb{F} 上的多项式, 对于任意 $a \in \mathbb{F}$, 存在 $g(x) \in \mathbb{F}[x]$ 使得

$$f(x) = (x - a)g(x) + f(a)$$



证明 不妨设 $f(x) = (x - a)g(x) + c$, 则 $f(a) = (a - a)g(a) + c$, 所以 $c = f(a)$ 。

结论 设 $f(x)$ 为域 \mathbb{F} 上的多项式, a 为 $f(x)$ 在域 \mathbb{F} 中的根的充要条件是 $(x - a) \mid f(x)$ 。

结论 设 $f(x)$ 为域 \mathbb{F} 上的 $n \geq 1$ 次多项式, 如果 a_1, a_2, \dots, a_m 为 $f(x)$ 在域 \mathbb{F} 中的 $m \geq 1$ 个不同的根, 则存在 $n - m$ 次多项式 $g(x) \in \mathbb{F}[x]$ 使得,

$$f(x) = (x - a_1)(x - a_2) \cdots (x - a_m)g(x)$$

结论 设 $f(x)$ 为域 \mathbb{F} 上的 $n \geq 1$ 次多项式, 则 $f(x)$ 在 \mathbb{F} 的任意扩域中, 不同根的个数都不会超过 n 。

3.6.2 扩域的构造

定理 3.15

设 $f(x)$ 为域 \mathbb{F} 上的 $n \geq 1$ 次不可约多项式



3.7 有限域的乘法群

3.7.1 有限域的乘法群

3.7.2 循环群的结构

定理 3.16

设 $\langle a \rangle$ 是由 a 生成的 n 阶的循环群, 试证明:

- (1) $\langle a \rangle$ 的子群都是循环群;
- (2) 对于任意正整数 $a \mid n$, $\langle a \rangle$ 存在唯一的 d 元子群;
- (3) 若整数 s, t 不全为 0, 则 $\langle a^s, a^t \rangle = \langle a^{(s,t)} \rangle$ 。



证明

(1) 设 G 是 $\langle a \rangle$ 任一子群, 如果 G 是单位元群, 结论成立。

否则 G 由 $a^i, 0 \leq i < n$ 中的一部分组成, 可设 G 中 a 的最小正幂为 a^m , 则根据 G 中乘法的封闭性, 那么

$\langle a^m \rangle$ 是 G 的子群, 且为循环群。

下面证明 $G = \langle a^m \rangle$

对于 $\forall a^k \in G, k \in \mathbb{Z}$, 设 $k = qm + r, 0 \leq r < m$

$$a^r = a^k (a^{-m})^q \in G \Rightarrow r = 0,$$

$$m \mid k, a^k = a^{mq} \in \langle a^m \rangle, G \subseteq \langle a^m \rangle.$$

由此说明: $\langle a \rangle$ 的子群 G 是由 G 中 a 的最小正幂 a^m 生成的循环群。

(2) 存在性: 对于 $d \mid n$, 令 $m = \frac{n}{d}$, 因为 $\text{ord}(a^m) = \frac{n}{(m, n)} = \frac{n}{m} = d$, 所以群 $\langle a^m \rangle$ 即为 d 阶子群。

唯一性: 设 G 是 $\langle a \rangle$ 的任一 d 阶子群, 该群中 a 的最小正幂为 a^m , 由 (1) 的证明, $G = \langle a^m \rangle$, 又因为 $a^n = e \in G$, 所以, 由 (1), $m \mid n$ 因此 a^m 的阶为 $\frac{n}{m} = d$, 所以 $m = \frac{n}{d}$ 。

由此说明, $\langle a \rangle$ 的所有 d 阶子群均由同一 a^m 生成, 它们是唯一的。

(3) $\langle a^s, a^t \rangle = \{a^{sx+ty} \mid x, y \in \mathbb{Z}\}$,

例题 3.4 试求域 $\mathbb{Z}_2[x]_{x^6+x+1}$ 中包含多项式 x^2+x+1 的根的最小子域。

解

第 4 章

4.1 勒让德符号

定义 4.1

设 m 是正整数, 若同余式

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

有解, 则 a 称作模 m 的二次剩余 (或平方剩余), 否则, a 称作模 m 的二次非剩余 (或平方非剩余)

1. 模 m 的同余式可以转化成模 p 的同余式



定义 4.2

设 p 是素数, 定义勒让德 (Legendre) 符号如下:



例题 4.1 对于素数 7, 因为 $(1)^2 \equiv 1(2)^2 \equiv 4(3)^2 \equiv 2 \pmod{7}$, 所以

$$\left(\frac{1}{7}\right)$$

4.1.1 欧拉判别法则

设 p 是素数, 求同余式 $x^2 \equiv a \pmod{p}$ 的解可以看成是在有限域 \mathbb{Z}_p 中求多项式 $x^2 - a$ 的根。

定理 4.1 (欧拉判别法则)

设 p 是奇素数, 则对于任意整数 a , $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ 。

