信息安全的数学基础

——AUST 期末复习真传

anyunyeyi

2026 年 2 月 16 日

前言

本文档第一版初稿写于 2025 年信安数学考试前一晚.

文档章节知识结构参考 CSDN 用户 Nebula_E_Zh 与往年试卷内容，定义及例题选自课本《信息安全的数学基础》（第 2 版）（陈恭亮）及其配套 PPT.

感谢他整理的全网第一份信安数学复习资料，（这是一个信息安全数学基础总复习指南的链接：https://blog.csdn.net/Nebula_E_Zh/article/details/135713884，你可以点击它进行访问）.

本复习文档对第 8,9 章节的内容，有所取舍，根据 2023 年的试题只记录了置换群的计算，其余内容等待补充.

第二次更新:

记录于 2025 年信安数学考试后，试卷结构改为 9 题，其中同余式求解内容的分值占比增加，相较于去年，增加的分值用来替换第一章整除的基础知识.

AB 卷的区别在于群章节的考察，B 卷与往年一致为置换群的简单计算，A 卷的则不同于 2007,2023 年试卷. 不熟悉课本的可以选择放弃，（10 分）. 剩下部分约有 40-50 分的内容为课本例题或书后习题，其余为数据改编. 第四五章节为难点内容，复习时需要着重考量.

anyunyeyi

2026 年 2 月 16 日

目录

第一章　整数的可除性

1.1　广义欧几里得算法

例 1.1.1. 设 $a = 169$, $b = 121$, 计算 (a, b).

解 利用广义欧几里得除法，有

$$\begin{aligned} 169 &= 1 \cdot 121 + 48, \\ 121 &= 2 \cdot 48 + 25, \\ 48 &= 1 \cdot 25 + 23, \\ 25 &= 1 \cdot 23 + 2, \\ 23 &= 11 \cdot 2 + 1, \\ 2 &= 2 \cdot 1 + 0. \end{aligned}$$

所以，$(169, 121) = 1$.

1.2　贝祖系数

例 1.2.1. 设 $a = 169$, $b = 121$, 求整数 s, t, 使得

$$s \cdot a + t \cdot b = (a, b).$$

解 由例 1.1.1, 有

$$\begin{aligned}
1 &= (-11)\cdot 2 + 23\\
&= (-11)\cdot((-1)\cdot 23+25) + 23\\
&= 12\cdot((-1)\cdot 25+48) + (-11)\cdot 25\\
&= (-23)\cdot((-2)\cdot 48+121) + 12\cdot 48\\
&= 58\cdot((-1)\cdot 121+169) + (-23)\cdot 121\\
&= 58\cdot 169 + (-81)\cdot 121.
\end{aligned}$$

因此，整数 $s=58, t=-81$ 满足 $s\cdot a+t\cdot b=(a,b)$.

1.3　素因数分解求最大公因数，最小公倍数

定义 1.3.1.

$$[a,b]=\frac{a\cdot b}{(a,b)}$$

（最小公倍数 = 两个数的乘积/最大公因数）

例 1.3.2. 设 $a=79720245000=2^3\cdot 5^4\cdot 11^6\cdot 3^2\cdot 7^0$, $b=9318751596=2^2\cdot 5^0\cdot 11^3\cdot 3^6\cdot 7^4$.

取

$$a'=2^3\cdot 5^4\cdot 11^6,\quad b'=3^6\cdot 7^4,\quad (a',b')=1,$$

则有

$$a'\cdot b'=2^3\cdot 5^4\cdot 11^6\cdot 3^6\cdot 7^4=[a,b].$$

第二章　同余

2.1　星期几问题

例 2.1.1. 2003 年 5 月 9 日是星期五，问第 2^{2003} 天是星期几？

解 因为

$$2^1 \equiv 2 \pmod 7, \quad 2^2 \equiv 4 \pmod 7, \quad 2^3 = 8 \equiv 1 \pmod 7,$$

又 $2003 = 667 \cdot 3 + 2$, 所以

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

故第 2^{2003} 天是星期二.

2.2　欧拉函数

定义 2.2.1. $\varphi =$ 模 m 的简化剩余系的元素个数

引理 2.2.2. 利用标准因数分解式计算欧拉函数: 设 m, n 是互素的两个正整数，则 $\varphi(m \cdot n) = \varphi(m)\varphi(n)$

2.3　欧拉小定理和费马小定理

定义 2.3.1. ***(Euler)*** 设 m 是大于 *1* 的整数. 如果 a 是满足 $(a, m) = 1$ 的整数，则

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

定义 2.3.2. ***(Fermat)*** 设 p 是一个素数，则对任意整数 a，有

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

注意： 欧拉定理和费马小定理的条件不同，欧拉定理中 m 是整数，费马小定理中 p 是素数.

2.4　模重复平方算法

例 2.4.1. 计算 $468^{237} \pmod{667}$.

解 设 $m = 667$, $b = 468$. 令 $a = 1$. 将 237 写成二进制，

$$237 = 1 + 2^2 + 2^3 + 2^5 + 2^6 + 2^7.$$

运用模重复平方法，依次计算如下：

1. $n_0 = 1$. 计算

$$a_0 = a \cdot b \equiv 468, \quad b_1 \equiv b^2 \equiv 248 \pmod{667}.$$

2. $n_1 = 0$. 计算

$$a_1 = a_0 \equiv 468, \quad b_2 \equiv b_1^2 \equiv 140 \pmod{667}.$$

3. $n_2 = 1$. 计算

$$a_2 = a_1 \cdot b_2 \equiv 154, \quad b_3 \equiv b_2^2 \equiv 257 \pmod{667}.$$

4. $n_3 = 1$. 计算

$$a_3 = a_2 \cdot b_3 \equiv 225, \quad b_4 \equiv b_3^2 \equiv 16 \pmod{667}.$$

5. $n_4 = 0$. 计算

$$a_4 = a_3 \equiv 225, \quad b_5 \equiv b_4^2 \equiv 256 \pmod{667}.$$

6. $n_5 = 1$. 计算

$$a_5 = a_4 \cdot b_5 \equiv 238, \quad b_6 \equiv b_5^2 \equiv 170 \pmod{667}.$$

7. $n_6 = 1$. 计算

$$a_6 = a_5 \cdot b_6 \equiv 440, \quad b_7 \equiv b_6^2 \equiv 219p \mod 667.$$

8. $n_7 = 1$. 计算

$$a_7 = a_6 \cdot b_7 \equiv 312 \pmod{667}.$$

最后，计算出

$$468^{237} \equiv 312 \pmod{667}.$$

2.5　剩余类，完全剩余系和简化剩余系

定义 2.5.1.　*1.* 剩余类：$mod\, m$ 同余的整数的集合.

2. 完全剩余系：有 m 个元素，两两不同余.

3. 简化剩余系：在完全剩余系的基础上去掉和 m 不互素的元素.

例 2.5.2. 设 m 是一个正整数，则

(i) $0, 1, \cdots, m-1$ 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) $1, \cdots, m-1, m$ 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) $-(m-1), \cdots, -1, 0$ 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) $-m, -(m-1), \cdots, -1$ 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，

$$-\frac{m}{2}, -\frac{m-2}{2}, \cdots, -1, 0, 1, \cdots, \frac{m-2}{2}$$

或

$$-\frac{m-2}{2}, \cdots, -1, 0, 1, \cdots, \frac{m-2}{2}, \frac{m}{2}$$

是模 m 的一个完全剩余系；当 m 分别为奇数时，

$$-\frac{m-1}{2}, \cdots, -1, 0, 1, \cdots, \frac{m-1}{2}$$

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.

第三章　同余式

3.1　求解一次同余式

定义 3.1.1. 设 m 是一个正整数，a 是满足 $m \nmid a$ 的整数，则一次同余式

$$ax \equiv 1 \pmod{m}$$

有解的充分必要条件是 $(a, m) = 1$. 而且，当上述同余式有解时，其解是唯一的.

引理 3.1.2. 解的形式

$$x = x_0 + t * \frac{m}{(a, m)} \pmod{m}$$

其中 x_0 为特解，$t = 0, 1, \ldots, (a, m) - 1$.

例 3.1.3. 求解一次同余式

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

解 首先，计算最大公因数 $(33, 77) = 11$，并且有 $(33, 77) = 11 \mid 22$，所以原同余式有解.

其次，运用广义欧几里得除法，求出同余式

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

的一个特解 $x_0' \equiv 5 \pmod{7}$.

再次，写出同余式

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

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

最后，写出原同余式的全部解

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

或者

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

3.2　中国剩余定理

引理 3.2.1. 核心公式

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

例 3.2.2. 求解同余式组

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

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

$M_1 = 6 \cdot 7 \cdot 11 = 462, \quad M_2 = 5 \cdot 7 \cdot 11 = 385, M_3 = 5 \cdot 6 \cdot 11 = 330, \quad M_4 = 5 \cdot 6 \cdot 7 = 210.$

分别求解同余式

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

得到

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

故同余式组的解为

$$\begin{aligned} x &\equiv b_1 \cdot 3 \cdot 462 + b_2 \cdot 1 \cdot 385 + b_3 \cdot 1 \cdot 330 + b_4 \cdot 1 \cdot 210 \\ &\equiv b_1 \cdot 1386 + b_2 \cdot 385 + b_3 \cdot 330 + b_4 \cdot 210 \pmod{2310}. \end{aligned}$$

注意: 每个同余式 mod 的数之间一定是互素的.

3.3　求解高次同余式及其提升

定义 3.3.1. 设 $m_1, \ldots, m_k$ 两两互素, $m = m_1 \cdots m_k$. 则

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

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

证设 x_0 是同余式 *(1)* 的解, 则 $f(x_0)\equiv 0\ (mod\, m)$. 从而 $f(x_0)\equiv 0\ (mod\, m_i),\quad i=1,\ldots,k$. 即 x_0 是同余式组 *(2)* 的解.

反过来, 设 $f(x_0)\equiv 0\ (mod\, m_i),\quad i=1,\ldots,k$, 则有 $f(x_0)\equiv 0\ (mod\, m)$. 即同余式组 *(2)* 的解 x_0 也是同余式 *(1)* 的解.

设 $f(x)\equiv 0\ (mod\, m_i)$ 的解是 $b_i,\ i=1,\ldots,k$. 则同余式组

$$\begin{cases} x\equiv b_1\ (mod\, m_1), \\ \quad\cdots \\ x\equiv b_k\ (mod\, m_k) \end{cases}$$

的解是 $x\equiv b_1\cdot M_1'\cdot M_1+\cdots+b_k\cdot M_k'\cdot M_k\ (mod\, m)$.

因为 $f(x)\equiv f(b_i)\equiv 0\ (mod\, m_i),\quad i=1,\ldots,k,$

所以 x 也是 $f(x)\equiv 0\ (mod\, m)$ 的解.

故 x 随 b_i 遍历 $f(x)\equiv 0\ (mod\ m_i)$ 的所有解 $(i=1,\ldots,k,)$ 而遍历 $f(x)\equiv 0\ (mod\, m)$ 的所有解, 即

$$\begin{cases} f(x)\equiv 0\ (mod\, m_1), \\ \quad\cdots \\ f(x)\equiv 0\ (mod\, m_k) \end{cases}$$

的解数为 $T=T_1\cdots T_k$.

例 3.3.2. 解同余式 $f(x)\equiv x^4+2x^3+8x+9\equiv 0\ (mod\ 35)$.

解 由定义 3.3.1 知原同余式等价于同余式组

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

直接验算,

$f(x)\equiv 0\ (mod\ 5)$ 的解为 $x\equiv 1,4\ (mod\ 5)$,

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

根据中国剩余定理, 可求得同余式组

$$\begin{cases} x\equiv b_1\ (mod\ 5) \\ x\equiv b_2\ (mod\ 7) \end{cases}$$

的解为 $x \equiv 3 \cdot 7 \cdot b_1 + 3 \cdot 5 \cdot b_2 \ (mod\ 35)$.

故原同余式的解为 $x \equiv 31, 26, 6, 24, 19, 34 \ (mod\ 35)$, 共 $2 \cdot 3 = 6$ 个. 事实上,

$$\begin{aligned} &1 \cdot 21 + 3 \cdot 15 = 66 \equiv 31, \quad 4 \cdot 21 + 3 \cdot 15 = 129 \equiv 24, \\ &1 \cdot 21 + 5 \cdot 15 = 96 \equiv 26, \quad 4 \cdot 21 + 5 \cdot 15 = 159 \equiv 19, \\ &1 \cdot 21 + 6 \cdot 15 = 111 \equiv 6, \quad 4 \cdot 21 + 6 \cdot 15 = 174 \equiv 34. \end{aligned}$$

引理 3.3.3. 因为

$$m = \prod_p p^\alpha,$$

所以要求解同余式　$f(x) \equiv 0 \ (mod\ m)$,　只须求解同余式　$f(x) \equiv 0 \ (mod\ p^\alpha)$.

我们讨论 p 为素数时,

$$f(x) \equiv 0 \ (mod\ p^\alpha) \tag{1}$$

的解法.

设 $f(x) = a_n x^n + \cdots + a_2 x^2 + a_1 x + a_0$ 为整系数多项式, 我们记

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

称 $f'(x)$ 为 $f(x)$ 的导式.

提升路线图:

$$\begin{array}{ll} f(x) \equiv 0 \ (mod\ p^\alpha) & x \equiv x_\alpha = x_{\alpha-1} + t_{\alpha-1} \cdot p^{\alpha-1} \ (mod\ p^\alpha) \\ \vdots & \\ f(x) \equiv 0 \ (mod\ p^2) & x \equiv x_i = x_{i-1} + t_{i-1} \cdot p^{i-1} \ (mod\ p^i) \\ \uparrow & \\ f(x) \equiv 0 \ (mod\ p^{i-1}) & x \equiv x_{i-1} \ (mod\ p^{i-1}) \\ \vdots & \\ f(x) \equiv 0 \ (mod\ p^2) & x \equiv x_2 = x_1 + t_1 \cdot p \ (mod\ p^2) \\ \uparrow & \\ f(x) \equiv 0 \ (mod\ p) & x \equiv x_1 \ (mod\ p) \end{array}$$

定义 3.3.4. 设 $x \equiv x_1 \ (mod\ p)$ 是同余式

$$f(x) \equiv 0 \ (mod\ p) \tag{2}$$

的一个解, 且

$$(f'(x_1), p) = 1,$$

则同余式 *(1)* 有解

$$x \equiv x_\alpha \ (mod\ p^\alpha), \tag{3}$$

其中 x_α 由下面关系式递归得到:

$$x_i \equiv x_{i-1} + t_{i-1} \cdot p^{i-1} \ (mod\ p^i), \quad i = 2, \ldots, \alpha, \tag{4}$$

这里

$$t_{i-1} \equiv \frac{-f(x_{i-1})}{p^{i-1}} \cdot (f'(x_1)^{-1} \ (mod\ p)) \ (mod\ p), \quad i = 2, \ldots, \alpha. \tag{5}$$

例 3.3.5. 求解同余式 $f(x) \equiv x^4 + 7x + 4 \equiv 0 \ (mod\ 27)$.

解 对于 $f(x)$, 有 $f'(x) \equiv 4x^3 + 7 \ (mod\ 27)$.

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

$$f(0) = 0^4 + 7 \cdot 0 + 4 \equiv 4 \equiv 1 \ (mod\ 3),$$
$$f(1) = 1^4 + 7 \cdot 1 + 4 = 12 \equiv 0 \ (mod\ 3),$$
$$f(2) = 2^4 + 7 \cdot 2 + 4 = 34 \equiv 1 \ (mod\ 3).$$

以 $x = 1 + 3t_1$ 代入 $f(x) \equiv 0 \ (mod\ 9)$, 可得

$$f(1) + 3t_1 f'(1) \equiv 0 \ (mod\ 9).$$

因为 $f(1) \equiv 3 \ (mod\ 9), \quad f'(1) \equiv 2 \ (mod\ 9)$, 所以上述同余式可写成

$$3 + 3t_1 \cdot 2 \equiv 0 \ (mod\ 9) \quad 或 \quad 2t_1 \equiv -1 \ (mod\ 3).$$

解得 $t_1 \equiv 1 \ (mod\ 3)$,

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

再以 $x = 4 + 9t_2$ 代入 $f(x) \equiv 0 \ (mod\ 27)$, 得

$$f(4) + 9t_2 f'(4) \equiv 0 \ (mod\ 27).$$

因为 $f(4) \equiv 18 \ (mod\ 27), \quad f'(4) \equiv 20 \ (mod\ 27)$, 所以上述同余式可写成

$$18 + 9t_2 \cdot 20 \equiv 0 \ (mod\ 27) \quad 或 \quad 2t_2 \equiv -2 \ (mod\ 3).$$

解得 $t_2 \equiv 2 \ (mod\ 3)$, 因此, 同余式 $f(x) \equiv 0 \ (mod\ 27)$ 的解为

$$x_3 \equiv 4 + 9t_2 \equiv 22 \ (mod\ 27).$$

3.4　求解素数模的同余式

例 3.4.1. 求解同余式

$$3x^{14}+4x^{13}+2x^{11}+x^9+x^6+x^3+12x^2+x\equiv 0\ (mod\ 7).$$

解： 由于模数 7 是质数，利用费马小定理（当 $x\not\equiv 0\pmod 7$ 时，$x^6\equiv 1\pmod 7$）简化指数.

1. 当 $x\equiv 0\pmod 7$ 时，代入得所有项为 0，故满足同余式，即 $x\equiv 0\pmod 7$ 是一个解.

2. 当 $x\not\equiv 0\pmod 7$ 时，指数可对 6 取模，简化多项式：

$$\begin{aligned}
3x^{14}&\equiv 3x^{14\mod 6}=3x^2 \pmod 7,\\
4x^{13}&\equiv 4x^{13\mod 6}=4x \pmod 7,\\
2x^{11}&\equiv 2x^{11\mod 6}=2x^5 \pmod 7,\\
x^9&\equiv x^{9\mod 6}=x^3 \pmod 7,\\
x^6&\equiv x^{6\mod 6}=x^0=1 \pmod 7,\\
x^3&\equiv x^{3\mod 6}=x^3 \pmod 7,\\
12x^2&\equiv 12x^{2\mod 6}=12x^2 \pmod 7,\\
x&\equiv x^{1\mod 6}=x \pmod 7.
\end{aligned}$$

合并同类项：

$$\begin{aligned}
&x^5\text{ 项}:2x^5,\\
&x^3\text{ 项}:x^3+x^3=2x^3,\\
&x^2\text{ 项}:3x^2+12x^2=15x^2\equiv 15-2\times 7=1\cdot x^2 \pmod 7,\\
&x\text{ 项}:4x+x=5x,\\
&\text{常数项}:1.
\end{aligned}$$

简化多项式为：

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

在模 7 下测试 $x=1,2,3,4,5,6$：

- $x=1$: $2(1)^5+2(1)^3+(1)^2+5(1)+1=11\equiv 4\not\equiv 0$,

- $x=2$: $2(32)+2(8)+4+5(2)+1\equiv 2(4)+2(1)+4+3+1=18\equiv 4\not\equiv 0$ (注: $32\equiv 4$, $8\equiv 1$, $10\equiv 3$),
- $x=3$: $2(243)+2(27)+9+5(3)+1\equiv 2(5)+2(6)+2+1+1=26\equiv 5\not\equiv 0$ (注: $243\equiv 5$, $27\equiv 6$, $9\equiv 2$, $15\equiv 1$),
- $x=4$: $2(1024)+2(64)+16+5(4)+1\equiv 2(2)+2(1)+2+6+1=15\equiv 1\not\equiv 0$ (注: $1024\equiv 2$, $64\equiv 1$, $16\equiv 2$, $20\equiv 6$),
- $x=5$: $2(3125)+2(125)+25+5(5)+1\equiv 2(3)+2(6)+4+4+1=27\equiv 6\not\equiv 0$ (注: $3125\equiv 3$, $125\equiv 6$, $25\equiv 4$, $25\equiv 4$),
- $x=6$: $2(7776)+2(216)+36+5(6)+1\equiv 2(6)+2(6)+1+2+1=28\equiv 0$ (注: $6\equiv -1$, $6^k\equiv(-1)^k$, 故 $6^5\equiv 6$, $6^3\equiv 6$, $6^2\equiv 1$, $30\equiv 2$).

因此, $x\equiv 6 \pmod 7$ 是解.

第四章　二次同余式与平方剩余

4.1　一般的二次同余式求解

例 4.1.1. 求解同余式 $x^2 \equiv 1219 \pmod{2310}$.

解 因为 $2310 = 5 \cdot 6 \cdot 7 \cdot 11$, 原同余式等价于同余式组

$$\begin{cases} x^2 \equiv 1219 \equiv 4 \pmod{5} \\ x^2 \equiv 1219 \equiv 1 \pmod{6} \\ x^2 \equiv 1219 \equiv 1 \pmod{7} \\ x^2 \equiv 1219 \equiv 9 \pmod{11} \end{cases},$$

分别求出三个同余式的解为

$$x = x_1 \equiv \pm 2 \pmod{5}, \quad x = x_2 \equiv \pm 1 \pmod{6},$$

$$x = x_3 \equiv \pm 1 \pmod{7}, \quad x = x_4 \equiv \pm 3 \pmod{7},$$

由韩信点兵例和中国剩余定理即得解为

$$x \equiv b_1 \cdot 1386 + b_2 \cdot 385 + b_3 \cdot 330 + b_4 \cdot 210 \pmod{2310},$$

$$x = 2\cdot 1386 + 1\cdot 385 + 1\cdot 330 + 3\cdot 210 = 4117 \equiv 1807 \pmod{2310},$$
$$x = 2\cdot 1386 + 1\cdot 385 + 1\cdot 330 + (-3)\cdot 210 = 2857 \equiv 547 \pmod{2310},$$
$$x = 2\cdot 1386 + 1\cdot 385 + (-1)\cdot 330 + 3\cdot 210 = 3457 \equiv 1147 \pmod{2310},$$
$$x = 2\cdot 1386 + 1\cdot 385 + (-1)\cdot 330 + (-3)\cdot 210 = 2197 \equiv 2197 \pmod{2310},$$
$$x = 2\cdot 1386 + (-1)\cdot 385 + 1\cdot 330 + 3\cdot 210 = 3347 \equiv 1037 \pmod{2310},$$
$$x = 2\cdot 1386 + (-1)\cdot 385 + 1\cdot 330 + (-3)\cdot 210 = 2087 \equiv 2087 \pmod{2310},$$
$$x = 2\cdot 1386 + (-1)\cdot 385 + (-1)\cdot 330 + 3\cdot 210 = 2687 \equiv 377 \pmod{2310},$$
$$x = 2\cdot 1386 + (-1)\cdot 385 + (-1)\cdot 330 + (-3)\cdot 210 = 1427 \equiv 1427 \pmod{2310},$$
$$x = (-2)\cdot 1386 + 1\cdot 385 + 1\cdot 330 + 3\cdot 210 = -1427 \equiv 883 \pmod{2310},$$
$$x = (-2)\cdot 1386 + 1\cdot 385 + 1\cdot 330 + (-3)\cdot 210 = -2687 \equiv 1933 \pmod{2310},$$
$$x = (-2)\cdot 1386 + 1\cdot 385 + (-1)\cdot 330 + 3\cdot 210 = -2087 \equiv 223 \pmod{2310},$$
$$x = (-2)\cdot 1386 + 1\cdot 385 + (-1)\cdot 330 + (-3)\cdot 210 = -3347 \equiv 1273 \pmod{2310},$$
$$x = (-2)\cdot 1386 + (-1)\cdot 385 + 1\cdot 330 + 3\cdot 210 = -2197 \equiv 113 \pmod{2310},$$
$$x = (-2)\cdot 1386 + (-1)\cdot 385 + 1\cdot 330 + (-3)\cdot 210 = -3457 \equiv 1163 \pmod{2310},$$
$$x = (-2)\cdot 1386 + (-1)\cdot 385 + (-1)\cdot 330 + 3\cdot 210 = -2857 \equiv 1763 \pmod{2310},$$
$$x = (-2)\cdot 1386 + (-1)\cdot 385 + (-1)\cdot 330 + (-3)\cdot 210 = -4117 \equiv 503 \pmod{2310}.$$

4.2　欧拉判别条件

讨论模为素数 p 的二次同余式

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

首先考虑模 p 的二次同余式有解的判别.

定义 4.2.1. （欧拉判别条件）设 p 是奇素数，$(a,p) = 1$，则

(i) a 是模 p 的平方剩余的充分必要条件是

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p};$$

(ii) a 是模 p 的平方非剩余的充分必要条件是

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

并且当 a 是模 p 的平方剩余时，同余式 (1) 恰有二解.

4.3　勒让德符号和二次互反律

定义 4.3.1. 设 p 是素数. 定义勒让德 *(Legendre)* 符号如下：

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

由此，对于 $(a,p)=1$，有

$$\left(\frac{a}{p}\right)=1 \iff x^2\equiv a \pmod p \text{ 有解}$$

$$\left(\frac{a}{p}\right)=-1 \iff x^2\equiv a \pmod p \text{ 无解}$$

定义 4.3.2. 设 p 是奇素数，则

(1) $\left(\frac{1}{p}\right)=1$;

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

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

定义 4.3.3. 设 p 是奇素数，则

(i) (周期性) $\left(\frac{a+p}{p}\right)=\left(\frac{a}{p}\right)$;

(ii) (完全可乘性) $\left(\frac{a\cdot b}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

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

定义 4.3.4. （二次互反律）若 p,q 是互素奇素数，则

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

4.4　二次同余式可解性判断及其求解

例 4.4.1. 求解同余式

$$x^2 \equiv 186 \pmod{401}.$$

解 因为 $a = 186 = 2 \cdot 3 \cdot 31$，计算勒让得符号

$$\left(\frac{2}{401}\right) = (-1)^{\frac{401^2-1}{8}} = 1, \quad \left(\frac{3}{401}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{401-1}{2}}\left(\frac{401}{3}\right) = \left(\frac{-1}{3}\right) = -1,$$

$$\left(\frac{31}{401}\right) = (-1)^{\frac{31-1}{2}\cdot\frac{401-1}{2}}\left(\frac{401}{31}\right) = \left(\frac{-2}{31}\right) = \left(\frac{-1}{31}\right)\left(\frac{2}{31}\right) = (-1)^{\frac{31-1}{2}}(-1)^{\frac{31^2-1}{8}} = -1,$$

所以

$$\left(\frac{186}{401}\right) = \left(\frac{2}{401}\right)\left(\frac{3}{401}\right)\left(\frac{31}{401}\right) = 1 \cdot (-1) \cdot (-1) = 1.$$

故原同余式有解. 对于奇素数 $p = 401$，将 $p-1$ 写成形式 $p - 1 = 400 = 2^4 \cdot 25$，其中 $t = 4$，$s = 25$ 是奇数.

(i) 任意选取一个模 401 平方非剩余 $n = 3$，即整数 $n = 3$ 使得 $\left(\frac{3}{401}\right) = -1$. 再令 $b := 3^{25} \equiv 268 \pmod{401}$.

(ii) 计算

$$x_3 := 186^{\frac{25+1}{2}} \equiv 103 \pmod{401}$$

以及 $a^{-1} \equiv 235 \pmod{401}$

(iii) 因为

$$(a^{-1}x_3^2)^2 \equiv 98^4 \equiv -1 \pmod{401},$$

令 $j_0 := 1$, $x_2 := x_3 b^{j_0} = 103 \cdot 268 \equiv 336 \pmod{401}$.

(iv) 因为

$$(a^{-1}x_2^2)^2 \equiv (-1)^2 \equiv 1 \pmod{401},$$

令 $j_1 := 0$, $x_1 := x_2 b^{j_1 2} = 336 \pmod{401}$.

(v) 因为

$$a^{-1}x_1^2 \equiv -1 \pmod{401},$$

令 $j_2 := 1$, $x_0 := x_1 b^{j_2 2^2} = 336 \cdot 268^4 \equiv 304 \pmod{401}$, 则 $x \equiv x_0 \equiv 304 \pmod{401}$ 满足同余式

$$x^2 \equiv 186 \pmod{401}.$$

第五章　原根与指标

5.1　指数与原根

定义 5.1.1. 设 $m>1$ 是整数，a 是与 m 互素的正整数，则使得

$$a^e \equiv 1 \pmod{m}$$

成立的最小正整数 e 叫做 a 对模 m 的 **指数**，记作 $\mathrm{ord}_m(a)$. 如果 a 对模 m 的指数是 $\varphi(m)$，则 a 叫做模 m 的 **原根**.

例 5.1.2. 设整数 $m=7$，这时 $\varphi(7)=6$. 有

$$1^1 \equiv 1, \qquad 2^3 = 8 \equiv 1, \qquad 3^3 = 27 \equiv -1,$$
$$4^3 \equiv (-3)^3 \equiv 1, \qquad 5^3 \equiv (-2)^3 \equiv -1, \qquad 6^2 \equiv (-1)^2 \equiv 1 \pmod{7}.$$

列成表为

a	1	2	3	4	5	6
$\mathrm{ord}_m(a)$	1	3	6	3	6	2

因此，$3,5$ 是模 7 的原根. 但 $2,4,6$ 不是模 7 的原根.

5.2　求模 p, p^2 的所有原根

定义 5.2.1. 设 $m>1$ 是整数. 如果模 m 存在一个原根 g，则模 m 有 $\varphi(\varphi(m))$ 个不同的原根

定义 5.2.2. 设 p 是奇素数，则模 p 的原根存在，且有 $\varphi(p-1)$ 个原根，其中 φ 为欧拉函数.

定义 5.2.3. 设 p 为奇素数, $p-1$ 的所有不同素因数是 $q_1,\cdots,q_s$，则 g 是模 p 原根的充要条件是

$$g^{\frac{p-1}{q_i}} \not\equiv 1 \pmod{m}, \quad i=1,\cdots,s. \tag{1}$$

定义 5.2.4. 设 g 是模 p 的一个原根, 则 g 或者 $g+p$ 是模 p^2 原根.

例 5.2.5. 求模 $p=43$ 的原根.

解 因为 $p-1=42=2\cdot 3\cdot 7$, $q_1=2$, $q_2=3$, $q_3=7$, 因此, $\frac{p-1}{q_1}=21$, $\frac{p-1}{q_2}=14$, $\frac{p-1}{q_3}=6$. 只需验证式 (1)，即 g^{21}, g^{14}, g^6 模 m 是否同余于 1. 对 $g=2,3,5$ 等，逐个验算.

$$\begin{aligned}
&2^2\equiv 4, \quad 2^4\equiv 16, \quad 2^6\equiv 64\equiv 21, \quad 2^7\equiv 21\cdot 2\equiv -1,\\
&2^{14}\equiv 1, \quad 3^2\equiv 9, \quad 3^4\equiv 81\equiv -5, \quad 3^6\equiv 9\cdot(-5)\equiv -2,\\
&3^7\equiv -6, \ 3^{14}\equiv(-6)^2\equiv 36, \ 3^{21}\equiv(-6)\cdot 36\equiv -1 \pmod{43}.
\end{aligned}$$

因此，$g=3$ 是模 $p=43$ 的原根.

进一步，当 $(d,p-1)=1$ 时，d 遍历模 $p-1=42$ 的简化剩余系：

$$1,5,11,13,17,19,23,25,29,31,37,41$$

共 $\varphi(p-1)=12$ 个数时，g^d 遍历模 43 的所有原根.

$$\begin{aligned}
&g^1\equiv 3, \quad g^5\equiv 28, \ g^{11}\equiv 30, \ g^{13}\equiv 12, \ g^{17}\equiv 26, \quad g^{19}\equiv 19, \ g^{23}\equiv 34,\\
&g^{25}\equiv 5, \ g^{29}\equiv 18, \ g^{31}\equiv 33, \ g^{37}\equiv 20, \ g^{41}\equiv 29 \pmod{43}.
\end{aligned}$$

例 5.2.6. 设 $m=43^2=1849$, 求模 m 的原根.

解由例 5.2.5，有 $g=3$ 是模 $p=43$ 的原根. 根据定义 5.2.4, 可知 $g=3$ 或者 $g+p=3+43=46$ 是模 $43^2=1849$ 的原根. 事实上, 我们有

$$g^{p-1}=3^{42}\equiv 87\equiv 1+2\cdot 43 \ (mod\ 43^2),$$

$$(g+p)^{p-1}=46^{40}\equiv 689\equiv 1+16\cdot 43 \ (mod\ 43^2).$$

因此, $g=3$ 和 $g+p=46$ 都是模 $m=p^2$ 的原根, 也都是模 $m=p^\alpha$ 的原根.

5.3　指标及其应用

定义 5.3.1. 设 m 是大于 *1* 的整数，g 是模 m 的一个原根. 设 a 是一个与 m 互素的整数，则存在唯一的整数 r 使得

$$g^r \equiv a \pmod{m}, \quad 1 \leqslant r \leqslant \varphi(m)$$

成立，这个整数 r 叫做以 g 为底的 a 对模 m 的一个 **指标**，记作 $r = \operatorname{ind}_g a$ *(或 $r \equiv \operatorname{ind} a$).*

定义 5.3.2. 设 m 是大于 *1* 的整数，g 是模 m 的一个原根. 设 a 是一个与 m 互素的整数，则同余式

$$x^n \equiv a \pmod{m}$$

有解的充分必要条件是

$$(n, \varphi(m)) \mid \operatorname{ind} a,$$

且在有解的情况下，解数为 $(n, \varphi(m))$.

例 5.3.3. 求解同余式

$$x^{12} \equiv 37 \pmod{41}.$$

解 因为

$$d = (n, \varphi(m)) = (12, \varphi(41)) = (12, 40) = 4,$$

$$\operatorname{ind} 37 = 32.$$

又 $4 \mid 32$，所以同余式有解. 现求解等价的同余式

$$12 \operatorname{ind} x \equiv \operatorname{ind} 37 \pmod{40}$$

或

$$3 \operatorname{ind} x \equiv 8 \pmod{10}.$$

得到

$$\operatorname{ind} x \equiv 6, 16, 26, 36 \pmod{40}.$$

查指标表得原同余式解

$$x \equiv 39, 18, 2, 23 \pmod{41}.$$

例 5.3.4. 作模 41 的指标表.

解 已知 $g=6$ 是模 $m=41$ 的原根, 直接计算 $g^r\ (mod\ m)$:

$$6^{40}\equiv 1,\quad 6^1\equiv 6,\quad 6^2\equiv 19,\quad 6^3\equiv 11,\quad 6^4\equiv 25,\quad 6^5\equiv 27,$$
$$6^6\equiv 39,\quad 6^7\equiv 29,\quad 6^8\equiv 10,\quad 6^9\equiv 19,\quad 6^{10}\equiv 32,\quad 6^{11}\equiv 28,$$
$$6^{12}\equiv 4,\quad 6^{13}\equiv 24,\quad 6^{14}\equiv 21,\quad 6^{15}\equiv 3,\quad 6^{16}\equiv 18,\quad 6^{17}\equiv 26,$$
$$6^{18}\equiv 33,\quad 6^{19}\equiv 34,\quad 6^{20}\equiv 40,\quad 6^{21}\equiv 35,\quad 6^{22}\equiv 5,\quad 6^{23}\equiv 30,$$
$$6^{24}\equiv 16,\quad 6^{25}\equiv 14,\quad 6^{26}\equiv 2,\quad 6^{27}\equiv 12,\quad 6^{28}\equiv 31,\quad 6^{29}\equiv 22,$$
$$6^{30}\equiv 9,\quad 6^{31}\equiv 13,\quad 6^{32}\equiv 37,\quad 6^{33}\equiv 17,\quad 6^{34}\equiv 20,\quad 6^{35}\equiv 38,$$
$$6^{36}\equiv 23,\quad 6^{37}\equiv 15,\quad 6^{38}\equiv 8,\quad 6^{39}\equiv 7\quad (mod\ 41).$$

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的数.

	0	1	2	3	4	5	6	7	8	9
0	0	40	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9
2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

例 5.3.5. 分别求整数 $a=28,18$ 以 $g=6$ 为底模 $m=41$ 的指标.

解根据模 41 的以原根 $g=6$ 的指标表, 我们查找十位数 2 所在的行, 个位数 8 所在的列, 交叉位置的数 11 就是 $ind_6 28=11$. 而查找十位数 1 所在的行, 个位数 8 所在的列, 交叉位置的数 16 就是 $ind_6 18=16$.

第六章　素性检验

6.1　各类定义及其应用

伪素数定义、Carmichael 数定义、Euler 伪素数定义、强伪素数的定义.

定义 6.1.1. 设 n 是一个奇合数. 如果整数 b, $(b,n)=1$ 使得同余式

$$b^{n-1} \equiv 1 \pmod{n}$$

成立，则 n 叫做对于基 b 的 **伪素数**.

例 6.1.2. 整数 $341 = 11 \cdot 31$, $561 = 3 \cdot 11 \cdot 17$, $645 = 3 \cdot 5 \cdot 43$ 都是对于基 $b = 2$ 的伪素数, 因为

$$2^{340} \equiv 1 \ (mod\ 341), \quad 2^{560} \equiv 1 \ (mod\ 561), \quad 2^{644} \equiv 1 \ (mod\ 645).$$

事实上, 我们有

$$\begin{cases} 2^{10} \equiv 1 \ (mod\ 11) \\ 2^{5} \equiv 1 \ (mod\ 31), \end{cases} \qquad \begin{cases} 2^{2} \equiv 1 \ (mod\ 3) \\ 2^{10} \equiv 1 \ (mod\ 11) \\ 2^{8} \equiv 1 \ (mod\ 17), \end{cases} \qquad \begin{cases} 2^{2} \equiv 1 \ (mod\ 3) \\ 2^{4} \equiv 1 \ (mod\ 5) \\ 2^{14} \equiv 1 \ (mod\ 43). \end{cases}$$

定义 6.1.3. 合数 n 称为 ***Carmichael*** 数，如果对所有的正整数 b, $(b,n)=1$，都有同余式

$$b^{n-1} \equiv 1 \pmod{n}$$

成立.

注 *Carmichael* 数 n 也可解释为这样一个正合数 n，它使得对所有的正整数 b, $(b,n)=1$, $n-1$ 都是序列 $u = \{u_k = b^k \mod n \mid k \geqslant 1\}$ 的周期.

例 6.1.4. 整数 $561 = 3 \cdot 11 \cdot 17$ 是一个 *Carmichael* 数.

证如果 $(b,561)=1$, 则 $(b,3)=(b,11)=(b,17)=1$. 根据 *Fermat* 小定理, 有

$$b^2\equiv 1\ (mod\ 3),\quad b^{10}\equiv 1\ (mod\ 11),\quad b^{16}\equiv 1\ (mod\ 17).$$

从而,

$$\begin{cases} b^{560}\equiv (b^2)^{280}\equiv 1\ (mod\ 3),\\ b^{560}\equiv (b^{10})^{56}\equiv 1\ (mod\ 11),\\ b^{560}\equiv (b^{16})^{35}\equiv 1\ (mod\ 17). \end{cases}$$

因此, 我们有　$b^{560}\equiv 1\ (mod\ 561)$.

定义 6.1.5. 设 n 是一个正奇合数. 设整数 b 与 n 互素. 如果整数 n 和 b 满足条件

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

则 n 叫做对于基 b 的 ***Euler* 伪素数**.

例 6.1.6. 设 $n=1105$, $b=2$. 我们分别计算得到:

$$2^{\frac{1105-1}{2}}\equiv 1\ (mod\ 1105)\quad 以及\quad \left(\frac{2}{1105}\right)=(-1)^{\frac{1105^2-1}{8}}=1.$$

因为

$$2^{\frac{1105-1}{2}}\equiv \left(\frac{2}{1105}\right)\ (mod\ 1105),$$

所以 *1105* 是一个对于基 *2* 的 *Euler* 伪素数.

定义 6.1.7. 设 n 是一个奇合数, 且有表示式 $n-1=2^st$, 其中 t 为奇数. 设整数 b 与 n 互素. 如果整数 n 和 b 满足条件

$$b^t\equiv 1\pmod n,$$

或者存在一个整数 r, $0\leqslant r<s$ 使得

$$b^{2^rt}\equiv -1\pmod n,$$

则 n 叫做对于基 b 的 **强伪素数**.

例 6.1.8. 整数 $n=2047=23\cdot 89$ 是对于基 $b=2$ 的强伪素数.

解因为

$$2^{2046/2}\equiv (2^{11})^{93}\equiv (2048)^{93}\equiv 1\ (mod\ 2047),$$

所以整数 *2047* 是对于基 $b=2$ 的强伪素数.

第七章　群与群的结构

7.1　循环群

例 7.1.1. 设 $\sigma=\begin{pmatrix}1&2&3&4&5&6\\6&5&4&2&1&3\end{pmatrix}$, $\tau=\begin{pmatrix}1&2&3&4&5&6\\5&6&4&2&3&1\end{pmatrix}$. 计算 $\sigma\tau,\tau\sigma,\sigma^{-1}$.

解: 将 τ 的像作为 σ 的像源，并依次对应，有

$$\begin{aligned}\sigma\cdot\tau&=\begin{pmatrix}1&2&3&4&5&6\\6&5&4&2&1&3\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\5&6&4&2&3&1\end{pmatrix}\\&=\begin{pmatrix}5&6&4&2&3&1\\1&3&2&5&4&6\end{pmatrix}\\&=\begin{pmatrix}1&2&3&4&5&6\\1&3&2&5&4&6\end{pmatrix}.\end{aligned}$$

$$\tau\cdot\sigma=\begin{pmatrix}6&5&4&2&1&3\\1&3&2&6&5&4\end{pmatrix}\begin{pmatrix}1&2&3&4&5&6\\6&5&4&2&1&3\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\1&3&2&6&5&4\end{pmatrix}.$$

$$\sigma^{-1}=\begin{pmatrix}6&5&4&2&1&3\\1&2&3&4&5&6\end{pmatrix}=\begin{pmatrix}1&2&3&4&5&6\\5&4&6&3&2&1\end{pmatrix}.$$

第八章　各章节习题精选

注意

大部分例题可以在参考答案中找到，其中四五章节的计算过于复杂，掌握例题即可，学有余力者可以自行练习.

八九章节内容可以参考离散数学中的讲解，着重掌握置换群的计算（送分题且大概率为考查内容）.

8.1　第一章

1. (28)

2. (29)

3. (32)

4. (50)

5. (51)

8.2　第二章

1. (1)

2. (6)

8.3　第三章

1. (1)

2. (2)

3. (3)

4. (12)

5. (13)

6. (14)

7. (15)

8. (23)

9. (24)

8.4　第六章

1. (1)

2. (3)

3. (5)

4. (9)

5. (14)

6. (16)

7. (17)

8.5　第九章

1. (1)