第 3 章　同余

同余是数论中极为重要的概念，在后面的第 6 和 7 章中也经常提及，如陪集和商群等概念．本章我们重点讨论整数的同余理论．

3.1　同余的概念和性质

在人们最开始学习整数除法的时候，可能比较关注于计算得到的商．但是，从这一节开始，我们将要把视角变化一下，关注于计算得到的余数．如果两个整数 a 和 b 同时为奇数或者同时为偶数，那么我们早就知道称它们具有相同的奇偶性，其充分必要条件是：$a-b$ 是偶数，即 $2\mid(a-b)$，换个说法就是 a 和 b 被 2 除的时候具有相同的余数．同余的理论就是从推广奇偶性这个概念开始的，只不过是奇偶性中整数 2 的角色被某个任意指定的正整数所替代．为此，我们先引入同余与同余式的概念．

定义 3.1.1　给定一个正整数 m，如果用 m 去除两个整数 a 和 b 所得的余数相同，则称 a 和 b 模 m **同余**，记作

$$a\equiv b\pmod m;\tag{3.1.1}$$

否则，称 a 和 b 模 m **不同余**，记作

$$a\not\equiv b\pmod m.$$

关系式(3.1.1)称为模 m 的同余式，或简称**同余式**.

例如，$26\equiv 2\pmod 3$，$63\equiv 3\pmod 5$，$23\equiv -5\pmod 7$.

定理 3.1.1　整数 a 和 b 模 m 同余的充要条件是 $m\mid a-b$.

证明　先证必要性．由 $a\equiv b\pmod m$，可设

$$a=mq_1+r,\quad b=mq_2+r,\quad 0\leqslant r<m,$$

则 $a-b=m(q_1-q_2)$，即 $m\mid a-b$.

再证充分性．设

$$a=mq_1+r_1,\quad 0\leqslant r_1<m,$$
$$b=mq_2+r_2,\quad 0\leqslant r_2<m,$$

则 $a-b=m(q_1-q_2)+r_1-r_2$．由 $m\mid a-b$，可知 $m\mid r_1-r_2$，则 $m\mid\mid r_1-r_2\mid$．又因 $0\leqslant r_2<m$，所以 $-m<-r_2\leqslant 0$，与 $0\leqslant r_1<m$ 两个不等式相加，得到 $-m<r_1-r_2<m$，即 $\mid r_1-r_2\mid<m$，故 $\mid r_1-r_2\mid=0$，所以 $r_1=r_2$．定理得证.

于是，同余又可以定义如下，即若 $m\mid a-b$，则称 a 和 b 模 m 同余．根据整除的定义，我们可以很直观地给出另一个判别同余的充要条件.

定理 3.1.2　整数 a 和 b 模 m 同余的充要条件是存在一个整数 k 使得

$$a=b+km.$$

由同余的定义，可以得到整数之间的同余具有等价关系的性质，利用它可以快捷地判断两个整数 a 和 b 是否模 m 同余.

定理 3.1.3　同余关系是等价关系，即

(1) 自反性：$a\equiv a\pmod m$；

(2) 对称性：若 $a\equiv b\pmod m$，则 $b\equiv a\pmod m$；

(3) 传递性：若 $a\equiv b \pmod m$, $b\equiv c \pmod m$, 则 $a\equiv c \pmod m$.

证明 (1)和(2)的证明略.

(3) 由 $m\mid a-b$ 和 $m\mid b-c$, 得到 $m\mid[(a-b)+(b-c)]$, 即 $m\mid a-c$.

定理 3.1.4 设 a_1, a_2, b_1, b_2 为四个整数, 如果

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

则有

(1) $a_1x+a_2y\equiv b_1x+b_2y \pmod m$, 其中 x, y 为任意整数;

(2) $a_1a_2\equiv b_1b_2 \pmod m$;

(3) $a_1^n\equiv b_1^n \pmod m$, 其中 $n>0$.

证明 (1) 由于 $m\mid a_1-b_1$, $m\mid a_2-b_2$, 故 $m\mid x(a_1-b_1)+y(a_2-b_2)$, 又

$$x(a_1-b_1)+y(a_2-b_2)=(a_1x+a_2y)-(b_1x+b_2y),$$

则 $m\mid(a_1x+a_2y)-(b_1x+b_2y)$, 即 $a_1x+a_2y\equiv b_1x+b_2y \pmod m$.

(2) 由于 $m\mid a_1-b_1$, $m\mid a_2-b_2$, 故 $m\mid a_2(a_1-b_1)+b_1(a_2-b_2)$, 又

$$a_2(a_1-b_1)+b_1(a_2-b_2)=a_1a_2-b_1b_2,$$

则 $m\mid a_1a_2-b_1b_2$, 即 $a_1a_2\equiv b_1b_2 \pmod m$.

(3) 由(2)可证.

例 3.1.1 求 $3^{2\,006}$, $3^{2\,009}$ 写成十进制数时的个位数.

解 由于

$$3^2\equiv 9 \pmod{10}, \quad 3^4\equiv 1 \pmod{10},$$

故可得 $3^{4\times 501}\equiv 1 \pmod{10}$. 又 $2\,006=4\times 501+2$, 故此可得 $3^{2\,006}\equiv 9 \pmod{10}$. 所以 $3^{2\,006}$ 写成十进制数时的个位数是 9.

同样地, 由于

$$3^1\equiv 3 \pmod{10}, \quad 3^4\equiv 1 \pmod{10},$$

故可得 $3^{4\times 502}\equiv 1 \pmod{10}$. 又 $2\,009=4\times 502+1$, 因此可得 $3^{2\,009}\equiv 3 \pmod{10}$. 所以 $3^{2\,009}$ 写成十进制数时的个位数是 3.

例 3.1.2 已知 2009 年 3 月 9 日是星期一, 问之后第 2^{100} 天是星期几? 之后第 2^{200} 天呢?

解 由于

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

故可得 $2^{3\times 33}\equiv 1 \pmod 7$. 又 $100=3\times 33+1$, 则 $2^{100}\equiv 2 \pmod 7$. 所以之后第 2^{100} 天是星期三.

同样地, 由于

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

故可得 $2^{3\times 66}\equiv 1 \pmod 7$. 又 $200=3\times 66+2$, 则 $2^{200}\equiv 4 \pmod 7$. 所以之后第 2^{200} 天是星期五.

定理 3.1.5 设 $f(t)=a_nt^n+a_{n-1}t^{n-1}+\cdots+a_1t+a_0$ 与 $g(t)=b_nt^n+b_{n-1}t^{n-1}+\cdots+b_1t+b_0$ 是两个整系数多项式, 满足

$$a_i\equiv b_i \pmod m, \quad 0\leqslant i\leqslant n,$$

那么, 若 $x\equiv y \pmod m$, 则

$$f(x)\equiv g(y) \pmod m.$$

证明 由 $x\equiv y \pmod m$, 可得

$$x^i\equiv y^i \pmod m, \quad 0\leqslant i\leqslant n,$$

又 $a_i\equiv b_i \pmod m$, $0\leqslant i\leqslant n$, 将它们对应相乘, 则有

$$a_ix^i\equiv b_iy^i \pmod m, \quad 0\leqslant i\leqslant n,$$

将这些同余式左右对应相加, 可得

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\equiv b_ny^n+b_{n-1}y^{n-1}+\cdots+b_1y+b_0 \pmod m,$$

即 $f(x)\equiv g(y)\pmod m$.

例 3.1.3 证明正整数 n（十进制）能被 9 整除的充要条件是将 n 的各位数字相加所得之和能被 9 整除.

证明 n 可写为十进制表示式：

$$n = 10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10\, a_1 + a_0,\quad 0\leqslant a_i < 10.$$

因为 $10^i \equiv 1 \pmod 9$，$0\leqslant i\leqslant k$，所以

$$10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10a_1 + a_0 \equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod 9.$$

因此，

$$10^k a_k + 10^{k-1} a_{k-1} + \cdots + 10\, a_1 + a_0 \equiv 0 \pmod 9$$

的充要条件是

$$a_k + a_{k-1} + \cdots + a_1 + a_0 \equiv 0 \pmod 9.$$

命题得证.

例 3.1.4 证明：当 n 是奇数时，$2^n + 1$ 能被 3 整除；当 n 是偶数时，$2^n + 1$ 不能被 3 整除.

证明 因为 $2\equiv -1 \pmod 3$，故 $2^n \equiv (-1)^n \pmod 3$，于是

$$2^n + 1 \equiv (-1)^n + 1 \pmod 3.$$

因此，当 n 是奇数时，

$$2^n + 1 \equiv 0 \pmod 3,$$

即 $2^n + 1$ 能被 3 整除；当 n 是偶数时，

$$2^n + 1 \equiv 2 \pmod 3,$$

即 $2^n + 1$ 不能被 3 整除.

定理 3.1.6 若 $ac\equiv bc \pmod m$，且$(c, m) = d$，则 $a\equiv b \pmod{\frac{m}{d}}$.

证明 由 $m \mid c(a - b)$，可知 $\frac{m}{d} \mid \frac{c}{d}(a - b)$，又$(\frac{m}{d}, \frac{c}{d}) = 1$，于是 $\frac{m}{d} \mid a - b$，即

$$a\equiv b \pmod{\frac{m}{d}}.$$

例如，通过 $260\equiv 20 \pmod{30}$，$(10, 30) = 10$，可得 $26\equiv 2 \pmod 3$.

定理 3.1.7 若 $a\equiv b \pmod m$，则有 $ak\equiv bk \pmod{mk}$，其中 k 为正整数.

证明 由 $m \mid a - b$，可知 $mk \mid ak - bk$，即 $ak\equiv bk \pmod{mk}$.

例如，通过 $26\equiv 2 \pmod 3$，可得 $260\equiv 20 \pmod{30}$.

定理 3.1.8 若 $a\equiv b \pmod m$，且有正整数 d 满足 $d \mid m$，则 $a\equiv b \pmod d$.

证明 由 $m \mid a - b$，$d \mid m$，可知 $d \mid a - b$，即 $a\equiv b \pmod d$.

例如，通过 $260\equiv 20 \pmod{30}$，可得 $260\equiv 20 \pmod 3$.

定理 3.1.9 若 $a\equiv b \pmod{m_i}$，$i = 1, 2, \cdots, n$，则

$$a\equiv b \pmod{[m_1, m_2, \cdots, m_n]}.$$

证明 由 $m_i \mid a - b$，$i = 1, 2, \cdots, n$，可知$[m_1, m_2, \cdots, m_n] \mid a - b$，即 $a\equiv b \pmod{[m_1, m_2, \cdots, m_n]}$.

例如，通过 $260\equiv 20 \pmod{30}$，$260\equiv 20 \pmod{80}$，又$[30, 80] = 240$，可得 $260\equiv 20 \pmod{240}$.

定理 3.1.10 若 $a\equiv b \pmod m$，则$(a, m) = (b, m)$.

证明 由 $a\equiv b \pmod m$，可知存在整数 k 使得 $a = b + mk$，于是$(a, m) = (b, m)$.

以上我们介绍了同余的一些基本性质．同余是数论中一个十分重要的概念，并且应用领域十分广泛，尤其是随着近代密码学的发展，同余及其相关理论的重要性越发显现出来.

习题 3.1

A 组

1. (1) 求 $7^{2\,046}$ 写成十进制数时的个位数；

   (2) 求 $2^{1\,000}$ 的十进制表示中的末尾两位数字.

2. 证明正整数 n（十进制）能被 3 整除的充要条件是将 n 的各位数字相加所得之和能被 3 整除.

3. 证明如果 $u \equiv v \pmod{n}$，那么 $(u, n) = (v, n)$.

4. 求 $1^5+2^5+3^5+\cdots+99^5$ 之和被 4 除的余数.

B 组

1. 证明：设 $f(x)$是整系数多项式，并且 $f(1)$，$f(2)$, …，$f(m)$都不能被 m 整除，则 $f(x) = 0$ 没有整数解.

2. 计算 555^{555} 被 7 除的余数.

3.2 剩余类和剩余系

因为同余是一种整数集合上的等价关系，所以我们可利用同余关系把全体整数划分成若干个等价类，并将每个等价类中的整数作为一个整体来考虑，进而可以得到一些相关的性质.

定义 3.2.1 设 m 是一给定正整数，令 C_r 表示所有与整数 r 模 m 同余的整数所组成的集合，则任意一个这样的 C_r 叫作模 m 的一个**剩余类**. 一个剩余类中的任一数叫作该类的**代表元**.

我们可以用集合的形式来描述剩余类的定义，即

$$C_r = \{a \mid a \in \mathbb{Z},\ a \equiv r \pmod{m}\} = \{\cdots,\ r-2m,\ r-m,\ r,\ r+m,\ r+2m,\ \cdots\}.$$

显然 C_r 非空，因为 $r \in C_r$. 很多书中也使用 $[r]$ 来表示 C_r.

下面的定理将考察整数与剩余类的关系和剩余类之间的关系，尽管整数有无限多个，然而剩余类的个数是有限的.

定理 3.2.1 设 m 为一正整数，C_0，C_1，…，C_{m-1} 是模 m 的剩余类，则

(1) 任一整数恰包含在一个 C_r 中，这里 $0 \leqslant r \leqslant m-1$；

(2) $C_a = C_b$ 的充要条件是 $a \equiv b \pmod{m}$；

(3) C_a 与 C_b 的交集为空集的充要条件是 a 和 b 模 m 不同余.

证明 (1) 设 a 是任一整数，则存在唯一的整数 q，r 使得

$$a = qm + r, \quad 0 \leqslant r < m,$$

于是有 $a \equiv r \pmod{m}$，故 a 恰包含在 C_r 中.

(2) 先证必要性. 由于 $a \in C_a$，$b \in C_b$，又 $C_a = C_b$，显然有

$$a \equiv b \pmod{m}.$$

再证充分性. 对任意整数 $c \in C_a$，有

$$a \equiv c \pmod{m}.$$

又因为

$$b \equiv a \pmod{m},$$

故 $b \equiv c \pmod{m}$，即 $c \in C_b$，可见 $C_a \subseteq C_b$.

同理，对任意整数 $c \in C_b$，可证 $a \equiv c \pmod{m}$，即 $c \in C_a$，可见 $C_b \subseteq C_a$.

于是，$C_a = C_b$.

(3) 由(2)可知必要性成立. 下面证明充分性.

用反证法. 假设 C_a 与 C_b 的交集非空，即存在整数 c 满足 $c \in C_a$ 且 $c \in C_b$，则有

$$a \equiv c \pmod{m},$$

$$b \equiv c \pmod{m}.$$

于是，得到 $a \equiv b \pmod{m}$，与假设矛盾. 因此 C_a 与 C_b 的交集为空集.

由上面的定理我们可以看到，尽管在剩余类的定义中 C_r 的下标可以在整数范围内任意取值，但是 C_r 本身必然与 C_0，C_1，…，C_{m-1} 中的某一个集合实际上是同一个集合，只不过是给集合取的名字不同而已，换句话说，一共就存在 m 个不同的剩余类. 例如，

$$C_m = \{\cdots, -m, 0, m, 2m, 3m, \cdots\} = C_0,$$

因此，我们在考察剩余类的时候，往往只需要用到 C_0，C_1，…，C_{m-1} 这 m 个名字指称这 m 个集合就可以了.

定义 3.2.2 在模 m 的剩余类 C_0，C_1，…，C_{m-1} 中各取一代表元 $a_i \in C_i$，$i = 0, 1, \cdots, m-1$，则此 m 个数 a_0，a_1，…，a_{m-1} 称为模 m 的一个**完全剩余系**（又称**完系**）.

由此定义和定理 3.2.1 显然可得到如下定理.

定理 3.2.2 m 个整数 a_0，a_1，…，a_{m-1} 为模 m 的一个完全剩余系的充要条件是它们两两模 m 不同余.

例 3.2.1 以下是几个模 10 的完全剩余系：

0，1，2，3，4，5，6，7，8，9；

1，2，3，4，5，6，7，8，9，10；

10，21，22，23，34，45，46，67，78，99；

−9，−8，−7，−6，−5，−4，−3，−2，−1，0.

定义 3.2.3 对于正整数 m，

(1) 0，1，…，$m-1$ 为模 m 的一个完全剩余系，叫作模 m 的**最小非负完全剩余系**；

(2) 1，2，…，$m-1$，m 为模 m 的一个完全剩余系，叫作模 m 的**最小正完全剩余系**；

(3) $-(m-1)$，…，−1，0 为模 m 的一个完全剩余系，叫作模 m 的**最大非正完全剩余系**；

(4) $-m$，$-(m-1)$，…，−1 为模 m 的一个完全剩余系，叫作模 m 的**最大负完全剩余系**.

定理 3.2.3 设 k 是满足 $(k, m) = 1$ 的整数，b 是任意整数，若 a_0，a_1，…，a_{m-1} 是模 m 的一个完全剩余系，则 $ka_0 + b$，$ka_1 + b$，…，$ka_{m-1} + b$ 也是模 m 的一个完全剩余系. 即若 x 遍历模 m 的一个完全剩余系，则 $kx+b$ 也遍历模 m 的一个完全剩余系.

证明 由定理 3.2.2，我们只需要证明当 a_0，a_1，…，a_{m-1} 是模 m 的一个完全剩余系时，m 个整数

$$ka_0 + b, \quad ka_1 + b, \quad \cdots, \quad ka_{m-1} + b$$

模 m 两两不同余. 用反证法，假设存在 a_i 和 a_j（$i \neq j$）使得

$$ka_i + b \equiv ka_j + b \pmod{m},$$

则 $m \mid k(a_i - a_j)$. 由于 $(k, m) = 1$，所以 $m \mid a_i - a_j$，即 $a_i \equiv a_j \pmod{m}$，推出了矛盾，假设不成立. 于是，$ka_0 + b$，$ka_1 + b$，…，$ka_{m-1} + b$ 两两不同余，所以它们是模 m 的一个完全剩余系.

例如 0, 1, 2, 3, 4 为模 5 的一个完全剩余系，若令 $k = 7$，$b = 3$，则可以得到模 5 的另一个完全剩余系，即 3, 10, 17, 24, 31.

定理 3.2.4 若 x_i (i=0, 1, …, m_1-1)是模 m_1 的完全剩余系，y_j (j=0, 1, …, m_2-1)是模 m_2 的完全剩余系，其中 $(m_1, m_2) = 1$，则 $m_2 x_i + m_1 y_j$ (i=0, 1, …, m_1-1，j=0, 1, …, m_2-1)是模 $m_1 m_2$

的完全剩余系.

证明 同样由定理 3.2.2，我们只需要证明 $m_2x_i + m_1y_j$ (i=0, 1, …, m_1−1, j=0, 1, …, m_2−1)这 m_1m_2 个整数模 m_1m_2 两两不同余．用反证法，假设存在有序对(x_a, y_c)和(x_b, y_d) (0≤a, b≤m_1−1, 0≤c, d≤ m_2−1)，且(x_a, y_c)≠(x_b, y_d)，使得

$$m_2 x_a + m_1 y_c \equiv m_2 x_b + m_1 y_d \pmod{m_1m_2},$$

进而有

$$m_2 x_a + m_1 y_c \equiv m_2 x_b + m_1 y_d \pmod{m_1},$$

即

$$m_2 x_a \equiv m_2 x_b \pmod{m_1}.$$

于是 $m_1 | m_2(x_a - x_b)$，又$(m_1, m_2) = 1$，则 $m_1 | x_a - x_b$，即 $x_a \equiv x_b \pmod{m_1}$，由于它们来自于同一个模 m_1 的完全剩余系，所以 $x_a = x_b$．同理可证，$y_c = y_d$．说明$(x_a, y_c) = (x_b, y_d)$，与我们的假设矛盾．所以假设不成立，定理得证.

例 3.2.2 例如：0, 1, 2, 3, 4 是模 5 的完全剩余系, 0, 1, 2, 3 是模 4 的完全剩余系，则：

0 ⊲4+0 ⊲5=0,	0 ⊲4+1 ⊲5=5,	0 ⊲4+2 ⊲5=10,	0 ⊲4+3 ⊲5=15,
1 ⊲4+0 ⊲5=4,	1 ⊲4+1 ⊲5=9,	1 ⊲4+2 ⊲5=14,	1 ⊲4+3 ⊲5=19,
2 ⊲4+0 ⊲5=8,	2 ⊲4+1 ⊲5=13,	2 ⊲4+2 ⊲5=18,	2 ⊲4+3 ⊲5=23,
3 ⊲4+0 ⊲5=12,	3 ⊲4+1 ⊲5=17,	3 ⊲4+2 ⊲5=22,	3 ⊲4+3 ⊲5=27,
4 ⊲4+0 ⊲5=16,	4 ⊲4+1 ⊲5=21,	4 ⊲4+2 ⊲5=26,	4 ⊲4+3 ⊲5=31.

是模 20 的完全剩余系.

习题 3.2

A 组

1. 写出模 9 的一个完全剩余系，它的每个数都是奇数.
2. 写出模 9 的一个完全剩余系，它的每个数都是偶数.
3. 用模 5 和模 6 的完全剩余系，表示模 30 的完全剩余系.
4. 求模 11 的一个完全剩余系{ r_1, r_2, …, r_{11} }，使得 $r_i \equiv 1 \pmod 3$, 1≤ i≤11.

B 组

1. 证明当 m>2 时， $0^2, 1^2, \ldots, (m-1)^2$ 一定不是模 m 的完全剩余系.
2. 设有 m 个整数，它们都不属于模 m 的 0 的剩余类，证明其中必有两个数属于同一剩余类.

3.3 欧拉定理、费尔马小定理

定义 3.3.1 在模 m 的一个剩余类中，若有一个数与 m 互素，则该剩余类中所有数都与 m 互素，此时称该**剩余类与 *m* 互素**.

定义 3.3.2 设 m 是正整数，在 m 的所有剩余类中，与 m 互素的剩余类的个数称为 m 的**欧拉函数**，记为 $\varphi(m)$.

也可以说，欧拉函数 $\varphi(m)$ 是集合{0, 1, …, m−1}中与模 m 互素的整数的个数，显然，$\varphi(m)$ 是一个定义在正整数集上的函数.

例如，由于{0, 1, 2, 3, 4, 5}中与 6 互素的整数只有 1, 5，因此 $\varphi(6) = 2$．显然 $\varphi(1) = 1$，如果 p 为素数，则 $\varphi(p) = p$-1.

有了欧拉函数的定义，我们就可以导出著名的欧拉定理和费尔马小定理，欧拉定理揭示了整数模幂运算的本质特性，在数论理论和代数理论中有重要的地位，也是公钥密码学中的一个重要的基础理论问题．下面我们从正整数缩系的角度引入欧拉定理.

定义 3.3.3 设 m 是正整数，在与模 m 互素的 $\varphi(m)$ 个剩余类中，各取一个代表元

$$a_1,\ a_2,\ \cdots,\ a_{\varphi(m)},$$

它们所组成的集合叫作模 m 的一个**缩剩余系**（又称**简化剩余系**），简称为**缩系**（又称**简系**）.

例如，模 6 的缩系为{1, 5}．当 $m = p$ 为素数时，$\{1, 2, \cdots, p-1\}$是模 p 的缩系.

我们将 1 到 m-1 的范围内与 m 互素的整数构成的集合，称为 m 的最小正缩系（亦可称为最小非负缩系），在讨论缩系性质时，最小正缩系是用得比较多的一种缩系.

根据缩系的定义，不难得出以下定理.

定理 3.3.1 若 $a_1,\ a_2,\ \cdots,\ a_{\varphi(m)}$ 是 $\varphi(m)$ 个与 m 互素的整数，则 $a_1, a_2, \cdots, a_{\varphi(m)}$ 是模 m 的一个缩系的充要条件是它们两两模 m 不同余.

定理 3.3.2 若 a 是满足(a, m)=1 的整数, $a_1,\ a_2,\ \cdots,\ a_{\varphi(m)}$ 是模 m 的一个缩系，则 aa_1, $aa_2,\ \cdots,\ aa_{\varphi(m)}$也是模 m 的一个缩系．即若(a, m)=1, x 遍历模 m 的一个缩系，则 ax 也遍历模 m 的一个缩系.

证明 由于$(a,\ m)$ = 1 且 $(a_i,\ m)$ = 1 (i=1, 2, $\cdots$, $\varphi(m)$)，故$(aa_i,\ m)$ = 1 (i=1, 2, $\cdots$, $\varphi(m)$)．若存在 a_k 和 a_l $(1 \leqslant k, l \leqslant \varphi(m)$ 且 $k \neq l)$使得 $aa_k \equiv aa_l \pmod m$，由于(a, m) = 1，可得 $a_k \equiv a_l \pmod m$，这与条件 a_k 和 a_l 来自于模 m 的一个缩系是矛盾的．所以假设不成立，aa_1, $aa_2, \cdots, aa_{\varphi(m)}$, 两两模 m 不同余，且它们是 $\varphi(m)$ 个不同的整数．于是，$aa_1,\ aa_2,\ \cdots,\ aa_{\varphi(m)}$ 是模 m 的一个缩系.

例 3.3.1 设 a = 3，m = 8, 则(a, m) = 1，x 遍历模 m 的最小正缩系，则 $ax \pmod m$也遍历模 m 的最小正缩系，如下表所示：

x	1	3	5	7
$ax \pmod m$	3	1	7	5

定理 3.3.3 设 m 是大于 1 的整数，若 a 是满足(a, m) = 1 的整数，则

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

证明 设 $r_1,\ r_2,\ \cdots,\ r_{\varphi(m)}$是模 m 的一个缩系，则由定理 3.3.2 可知 $ar_1,\ ar_2,\ \cdots,\ ar_{\varphi(m)}$ 也是模 m 的一个缩系，所以对于第一个缩系的每一个元素，都在第二个缩系中存在唯一的元素与之在同一个剩余类中，所以

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

即

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

由于

$$(r_i,\ m) = 1\ （i = 1, 2, \cdots,\ \varphi(m)）,$$

故

$$(r_1 r_2 \cdots r_{\varphi(m)}, m) = 1.$$

于是，根据定理 3.1.6 可得

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

定理 3.3.3 又称作**欧拉定理**，通过这个定理可推出著名的**费马小定理**，即定理 3.3.4.

定理 3.3.4 若 p 是素数，则对任意整数 a，有

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

证明 若 a 不能被 p 整除，即$(a, p) = 1$，由欧拉定理，有

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

两端同乘 a 即得

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

若 a 能被 p 整除，则

$$a \equiv 0 \pmod{p}, \quad a^{p} \equiv 0 \pmod{p},$$

于是

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

定理得证.

关于欧拉定理和费尔马小定理的应用，我们举两个例子.

例 3.3.2 已知 x=10，计算 $115x^{15}+278x^{3}+12 \pmod 7$.

解 原式$\equiv 3x^{15}-2x^{3}-2 \pmod 7$

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

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

$\equiv 25 \pmod 7$

$\equiv 4 \pmod 7$.

例 3.3.3 求证对任意整数 n 有 $3n^{5}+5n^{3}+7n \equiv 0 \pmod{15}$.

证明 因为

$$3n^{5} \equiv 0 \pmod 3, \quad 5n^{3} \equiv 2n \pmod 3, \quad 7n \equiv n \pmod 3,$$

$$3n^{5} \equiv 3n \pmod 5, \quad 5n^{3} \equiv 0 \pmod 5, \quad 7n \equiv 2n \pmod 5.$$

所以

$$3n^{5}+5n^{3}+7n \equiv 0 \pmod 3,$$

$$3n^{5}+5n^{3}+7n \equiv 0 \pmod 5.$$

所以

$$3n^{5}+5n^{3}+7n \equiv 0 \pmod{15}.$$

在使用欧拉定理的时候，需要用到欧拉函数，下面来研究欧拉函数的求解问题.

定理 3.3.5 设 m_1, m_2 为互素的两个正整数，若 x_1, x_2 分别遍历模 m_1 和模 m_2 的缩系，则 $m_2x_1 + m_1x_2$ 遍历模 m_1m_2 的缩系.

证明 由$(m_1, m_2) = 1$，$(x_1, m_1) = 1$，$(x_2, m_2) = 1$，可知$(m_2x_1, m_1) = 1$，进而

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

同理，

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

于是，我们有

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

下面证明凡是与 m_1m_2 互素的数 a，必有

$$a \equiv m_2x_1 + m_1x_2 \pmod{m_1m_2}, \quad (x_1, m_1) = 1, (x_2, m_2) = 1.$$

由定理 3.2.4 可知有 x_1，x_2 使 $a \equiv m_2x_1 + m_1x_2 \pmod{m_1m_2}$，故只需证明当$(a, m_1m_2) = 1$ 时，$(x_1, m_1) = (x_2, m_2) = 1$．假设$(x_1, m_1) > 1$，则存在素数 p，使 $p \mid x_1$，$p \mid m_1$，又因为

$$a \equiv m_2x_1 + m_1x_2 \pmod{m_1m_2},$$

于是 $p \mid a$，故$(a, m_1m_2) > 1$，推出了矛盾．所以$(x_1, m_1) = 1$，同理可证$(x_2, m_2) = 1$.

最后，由定理 3.2.4 可知，所有的 $m_2x_1 + m_1x_2$ 两两模 m_1m_2 不同余．于是定理得证.

由定理 3.3.5，我们可推出以下定理，它反映了欧拉函数 $\varphi(m)$ 的性质，即 $\varphi(m)$ 为一积

性函数.

定理 3.3.6 设 m_1，m_2 为互素的两个正整数，则

$$\varphi(m_1m_2) = \varphi(m_1)\varphi(m_2).$$

证明 当 x_1 遍历模 m_1 的缩系时，其遍历的整数个数为 $\varphi(m_1)$．当 x_2 遍历模 m_2 的缩系时，其遍历的整数个数为 $\varphi(m_2)$．由定理 3.3.5，$m_2x_1 + m_1x_2$ 遍历模 m_1m_2 的缩系，其遍历的整数个数为 $\varphi(m_1)\varphi(m_2)$．又因为模 m_1m_2 的缩系的代表元个数为 $\varphi(m_1m_2)$，所以

$$\varphi(m_1m_2) = \varphi(m_1)\varphi(m_2).$$

定理得证.

以上定理很大程度地简化了求解欧拉函数值的过程．例如，如果求 $\varphi(55)$ 的值，以前我们需要列出所有小于 55 且与 55 互素的正整数，而利用定理 3.3.6，我们有

$$\varphi(55) = \varphi(5)\varphi(11) = 4\times10 = 40.$$

定理 3.3.7 设 m 有标准分解式

$$m = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s},\quad \alpha_i > 0,\quad i = 1,\ 2,\cdots,\ s,$$

则

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

证明 由 $\varphi(m)$ 的定义可知，$\varphi(p^\alpha)$ 等于 p^α 减去在 1，2，…，p^α 中与 p 不互素的数的个数．又由于 p 是素数，故 $\varphi(p^\alpha)$ 等于从 p^α 减去在 1，2，…，p^α 中被 p 整除的数的个数．在

$$1,\ \cdots,\ p,\ \cdots,\ 2p,\ \cdots,\ p^{\alpha-1}\cdot p$$

中，被 p 整除的数共有 $p^{\alpha-1}$ 个，故 $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$．由此，我们有

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

定理 3.3.7 告诉我们，已知一个大整数的所有素因子，可以很容易地求出它的欧拉函数值.

例 3.3.4 求φ(240).

解 $240 = 2^4\cdot3\cdot5$，所以，$\varphi(240) = 240(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5}) = 64$.

例 3.3.5 设正整数 n 是两个不同素数的乘积，如果已知 n 和欧拉函数 $\varphi(n)$ 的值，则可求出 n 的因子分解式.

证明 设此两个不同的素因子为 p 和 q，由于

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

我们有关于 p 和 q 的方程组：

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

于是，p 和 q 可由二次方程

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

求出.

例 3.3.6　设$\{x_1, x_2, \cdots, x_{\varphi(m)}\}$是模 m 的缩系，求证

$$(x_1x_2\cdots x_{\varphi(m)})^2 \equiv 1 \pmod{m}.$$

证明　记 $P = x_1x_2\cdots x_{\varphi(m)}$，则$(P, m) = 1$. 又记

$$y_i = \frac{P}{x_i},\ 1 \le i \le \varphi(m),$$

则$\{y_1, y_2, \cdots, y_{\varphi(m)}\}$也是模 m 的缩系，因此

$$\prod_{i=1}^{\varphi(m)} x_i \equiv \prod_{i=1}^{\varphi(m)} \frac{P}{x_i} \pmod{m},$$

再由欧拉定理，推出 $P^2 \equiv P^{\varphi(m)} \equiv 1 \pmod{m}$.

例 3.3.7　设 n 是正整数，记 $F_n = 2^{2^n} + 1$，求证 $2^{F_n} \equiv 2 \pmod{F_n}$.

证明　容易验证，当 $n \le 4$ 时 F_n 是素数，所以，由费尔马小定理可知结论显然成立.

当 $n \ge 5$ 时，有 $n + 1 < 2^n$，　$2^{n+1} \mid 2^{2^n}$. 记 $2^{2^n} = k2^{n+1}$，则

$$\begin{aligned} 2^{F_n} - 2 &= 2^{2^{2^n}+1} - 2 = 2(2^{2^{2^n}} - 1) = 2(2^{k2^{n+1}} - 1) \\ &= 2((2^{2^{n+1}})^k - 1) = 2Q_1(2^{2^{n+1}} - 1) = Q_2(2^{2^n} + 1), \end{aligned}$$

其中 Q_1 与 Q_2 是整数. 上式即是 $2^{F_n} \equiv 2 \pmod{F_n}$.

我们已经知道，F_5 是合数，因此，例 3.3.7 说明，费尔马小定理的逆定理不成立. 即若有整数 a，　且$(a, m) = 1$，使得

$$a^{m-1} \equiv 1 \pmod{m},$$

并不能保证 m 是素数.

习题 3.3

A 组

1. 写出 12 的最小正缩系.
2. 用模 5 和模 6 的缩系，表示模 30 的缩系.
3. 计算以下整数的欧拉函数

(1) 24;　(2) 64;　(3) 187;　(4) 360.

4. 利用费尔马小定理求解以下题目

(1) 求数 a（$0 \le a < 73$），使得 $a \equiv 9^{794} \pmod{73}$.

(2) 解方程 $x^{86} \equiv 6 \pmod{29}$.

(3) 解方程 $x^{39} \equiv 3 \pmod{13}$.

B 组

1. 证明 2, 2^2, 2^3, …, 2^{18} 是模 27 的一个缩系.
2. 证明如果 p 是奇素数, 那么

$$1^2 3^2 \cdots (p-4)^2 (p-2)^2 \equiv (-1)^{\frac{p+1}{2}} \pmod{p}.$$

3. 证明如果 a 是整数, 且$(a, 3) = 1$, 那么 $a^7 \equiv a \pmod{63}$.
4. 如果 $m>3$, 解释 $\varphi(m)$ 为什么总是偶数.
5. $\varphi(m)$ “经常”能被 4 整数, 列出所有 $\varphi(m)$ 不能被 4 整除的 m.
6. 编写计算正整数欧拉函数的程序.

3.4 扩展欧几里德算法、威尔逊定理

本节我们来研究模正整数的乘法运算的可逆性问题. 先看一个例子.

在模 10 的最小非负完全剩余系{0, 1, 2, 3, 4, 5, 6, 7, 8, 9}中, 在模 10 运算下有

$$1 \cdot 1 \equiv 1 \pmod{10},$$
$$3 \cdot 7 \equiv 1 \pmod{10},$$
$$9 \cdot 9 \equiv 1 \pmod{10},$$

即 $a \in \{1, 3, 7, 9\}$时, 存在一个整数 $a' \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, 使得 $aa' \equiv 1 \pmod{10}$, 而对于{0, 2, 4, 5, 6, 8}这个集合中的数, 不具有这种性质. 而集合{1, 3, 7, 9}恰好是 10 的最小正缩系. 一般地, 我们有以下定理:

定理 3.4.1 若 a 是满足$(a, m) = 1$ 的整数, 则存在唯一整数 a', $1 \leqslant a' < m$ 且$(a', m) = 1$, 使得

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

证明 （存在性）因为$(a, m) = 1$, 由定理 3.3.2, 当 x 遍历模 m 的最小正缩系时, ax 也遍历模 m 的一个缩系. 于是, m 的最小正缩系中存在整数 a', 使得 aa'和 1 在同一个剩余类中, 即

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

所以, m 的最小正缩系中存在整数 a', 使得 $aa' \equiv 1 \pmod{m}$,

（唯一性）若有整数 $a', a'', 1 \leqslant a', a'' < m$, 使得

$$aa' \equiv 1 \pmod{m} \text{且 } aa'' \equiv 1 \pmod{m}$$

则有 $a(a'-a'') \equiv 0 \pmod{m}$, 从而 $a'-a'' \equiv 0 \pmod{m}$. 故 $a'=a''$.证毕.

由定理 3.4.1 可以很容易地推出:

定义 3.4.1 对于正整数 m 和整数 a, 满足$(a, m) = 1$, 存在唯一一个 m 的剩余类, 其中每一个元素 a', 都会使 $aa' \equiv 1 \pmod{m}$成立, 此时称 a' 为 ***a* 模 *m* 的乘法逆元**, 记作 $a^{-1} \pmod{m}$.

乘法逆元的概念在公钥密码学中非常重要. 当 m 和 a 比较大时, 很难用定义来求 $a^{-1} \pmod{m}$. 下面我们来研究逆元的快速求法——扩展欧几里德算法, 它是在 2.2 节中介绍的欧几里德算法的基础上发展而来的.

定理 3.4.2 设 r_0, r_1 是两个正整数, 且 $r_0 > r_1$, 设 r_i $(i = 2, \ldots, n)$是使用欧几里德算法计算(r_0, r_1)时所得到的余数序列且 $r_{n+1} = 0$, 则可以使用如下算法求整数 s_n 和 t_n, 使得

$$(r_0, r_1) = s_n r_0 + t_n r_1.$$

这里 s_n 和 t_n 是如下递归定义的序列的第 n 项. 且

$$s_0 = 1, t_0 = 0$$

$$s_1 = 0,\ t_1 = 1$$

$$s_i = s_{i-2} - q_{i-1}s_{i-1},\ t_i = t_{i-2} - q_{i-1}t_{i-1},\ \text{其中}\ q_i = r_{i-1}/r_i,\ i = 2, 3, \ldots, n$$

证明　我们用归纳法证明 $r_i = s_i r_0 + t_i r_1,\ i = 0, 1, \ldots, n.$

当 $i = 0$ 时，　$s_i r_0 + t_i r_1 = s_0 r_0 + t_0 r_1 = r_0$，结论成立.

当 $i = 1$ 时，　$s_i r_0 + t_i r_1 = s_1 r_0 + t_1 r_1 = r_1$，结论成立.

假设 $r_i = s_i r_0 + t_i r_1$ 在 $i = 2, 3, \ldots, k\text{-}1$ 时成立，由欧几里德算法，$r_k = r_{k-2} - r_{k-1}q_{k-1}$，由归纳假设

$$\begin{aligned} r_k &= r_{k-2} - r_{k-1}q_{k-1} = (s_{k-2}r_0 + t_{k-2}r_1) - (s_{k-1}r_0 + t_{k-1}r_1)q_{k-1} \\ &= (s_{k-2} - s_{k-1}q_{k-1})r_0 + (t_{k-2} - t_{k-1}q_{k-1})r_1 \\ &= s_k r_0 + t_k r_1. \end{aligned}$$

由欧几里德算法有 $r_n = (r_0, r_1)$，所以，$(r_0, r_1) = r_n = s_n r_0 + t_n r_1$.

显然，当$(r_0, r_1) = 1$ 时，有 $s_n r_0 + t_n r_1 = 1$，于是定理 3.4.2 中 $s_n \equiv r_0^{-1} (\mathrm{mod}\ r_1)$且 $t_n \equiv r_1^{-1} (\mathrm{mod}\ r_0)$.

定理 3.4.2 中给出的求乘法逆元的算法称为**扩展欧几里德算法.**

例 3.4.1　求 550 模 1 769 的乘法逆元，以及 1 769 模 550 的乘法逆元.

解　我们可以列表计算定理 3.4.2 中系数 s_n 和 t_n，首先画出表头，并填写初始值如下：

i	r_i	q_i	s_i	t_i
0	1 769	-	1	0
1	550		0	1

然后计算 $q_1 = r_0/r_1 = 1\ 769/550 = 3$，并填入表中，再用公式 $s_2 = s_0 - q_1 s_1,\ t_2 = t_0 - q_1 t_1$ 计算 s_2 和 t_2 并填入表中，得到，

i	r_i	q_i	s_i	t_i
0	1 769	-	1	0
1	550	3	0	1
2	119		1	-3

重复以上步骤，直到 $r_i = 0$. 此时的 s_{i-1} 和 t_{i-1} 即为要求的系数 s_n 和 t_n.

i	r_i	q_i	s_i	t_i
0	1 769	-	1	0
1	550	3	0	1
2	119	4	1	-3
3	74	1	-4	13
4	45	1	5	-16
5	29	1	-9	29
6	16	1	14	-45
7	13	1	-23	74

8	3	4	37	-119
9	1	3	-171	550
	0		stop	stop

所以(1 769, 550) = 1, $550^{-1} \equiv 550 (\text{mod } 1\ 769)$, $1\ 769^{-1} \equiv -171 (\text{mod } 550) \equiv 379 (\text{mod } 550)$.
按照以上步骤，很容易写出用扩展欧几里德算法求乘法逆元的程序.

定理 3.4.3 设 p 为大于 2 的素数,证明:方程 $x^2 \equiv 1 \pmod{p}$的解只有 $x \equiv 1 \pmod{p}$和 $x \equiv -1 \pmod{p}$.

证明 由 $x^2 \equiv 1 \pmod{p}$有

$$x^2 - 1 \equiv 0 (\text{mod } p),$$

即

$$(x - 1)(x + 1) \equiv 0 (\text{mod } p),$$

因此有三种可能：

$$p|(x - 1)$$

或

$$p|(x + 1)$$

或

$$p|(x - 1) \text{且} p|(x + 1).$$

但若 $p|(x - 1)$且 $p|(x + 1)$，则存在两个整数 k 和 j，使得 $x + 1 = kp$, $x - 1 = jp$，两式相减得

$$2 = (k-j)p,$$

注意到 k 和 j 为整数, p 为大于 2 的整数, $2 = (k-j)p$ 不可能成立. 所有只能有 $p|(x - 1)$或 $p|(x + 1)$两种可能，由 $p|(x - 1)$可得 $x \equiv 1 (\text{mod } p)$，由 $p|(x + 1)$可得 $x \equiv -1 (\text{mod } p)$，所以方程方程 $x^2 \equiv 1 (\text{mod } p)$的解只有 $x \equiv 1 (\text{mod } p)$和 $x \equiv -1 (\text{mod } p)$.

定理 3.4.3 告诉我们，当 p 为大于 2 的素数时, p 的最小正缩系中模 p 的乘法逆元等于自身的元素只有 1 和 $p - 1$.

定理 3.4.4 设 p 是一个素数，则$(p-1)! \equiv -1 (\text{mod } p)$.

证明 若 $p = 2$，结论显然成立.

设 $p > 2$，由定理 3.4.1，对于每个整数 a, $1 \le a < p$，存在唯一的整数 a', $1 \le a' < p$，使得

$$aa' \equiv 1 (\text{mod } m).$$

而 $a = a'$充要条件是 a 满足

$$a^2 \equiv 1 (\text{mod } m).$$

根据定理 3.4.3，这时有 $a \equiv 1$ 或 $a \equiv m-1$.

因此，当 $a \in \{2, 3, \ldots, p-2\}$时，有 $a' \in \{2, 3, \ldots, p-2\}$. 我们将$\{2, 3, \ldots, p-2\}$中的 a 与 a'两两配对，得到

$$1 \cdot 2 \cdot \ldots \cdot (p-2) \cdot (p-1) \equiv 1 \cdot \prod_{a} aa' \cdot (p-1) (\text{mod } p)$$

$$\equiv 1 \cdot (p-1) (\text{mod } p)$$

$$\equiv -1 (\text{mod } p).$$

即$(p-1)! \equiv -1 (\text{mod } p)$，证毕.

这个定理又称为**威尔逊定理**.

习题 3.4

A 组

1. 计算 $8\cdot9\cdot10\cdot11\cdot12\cdot13 \pmod 7$.
2. 求 $229^{-1} \pmod{281}$.
3. 求 $3169^{-1} \pmod{3571}$.
4. 解方程 $105x + 121y = 1$.

B 组

1. 如果 p 为素数，且 $0 < k < p$，证明 $(p-k)!(k-1)! \equiv (-1)^k \pmod p$.
2. 编程判断两个正整数 m, n 是否互素，如果互素， 求出 $m^{-1} \pmod n$ 和 $n^{-1} \pmod m$.

3.5 线性同余方程

前面我们研究了同余的概念和一些性质，现在我们开始讨论在模 m 的情况下多项式方程的求解问题.

定义 3.5.1 设多项式

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0,$$

其中 $n>0$， a_i $(i = 0, 1, \cdots, n)$是整数，又设 $m>0$，则同余式

$$f(x) \equiv 0 \pmod m \tag{3.5.1}$$

称为模 m 的**同余方程**. 若 a_n 不能被 m 整除，则 n 称为 $f(x)$的**次数**，记为 $\deg f(x)$.

若 x_0 满足

$$f(x_0) \equiv 0 \pmod m,$$

则

$$x \equiv x_0 \pmod m$$

叫作同余方程(3.5.1)的**解**. 如果 $y_0 \equiv x_0 \pmod m$，那么必然有 $f(y_0) \equiv f(x_0) \equiv 0 \pmod m$，所以不同的解是指互不同余的解.

由定义可知，求解同余方程(3.5.1)，只要将 0, 1, …, $m-1$ 逐个代入式(3.5.1)中进行验算即可，但当 m 较大时，巨大的计算量难以令人满意.

例 3.5.1 求解同余方程 $x^4 + 3x^2 - 2x + 1 \equiv 0 \pmod 5$.

解 求解此模 5 的 4 次同余方程，可将 0, 1, 2, 3, 4 逐个代入，由于

$$2^4 + 3\times2^2 - 2\times2 + 1 = 25 \equiv 0 \pmod 5,$$

故 $x \equiv 2 \pmod 5$是该同余方程的解.

例 3.5.2 求解同余方程 $x^2 + 1 \equiv 0 \pmod 7$.

解 这是一个模 7 的 2 次同余方程，由于将 0, 1, …, 6 逐个代入方程中均不满足，故此同余方程无解.

下面我们讨论线性同余方程（一次同余方程）的求解问题.

定理 3.5.1 设 $m > 1$, $(a, m) = 1$，则同余方程

$$ax \equiv b \pmod m \tag{3.5.2}$$

有且仅有一个解 $x \equiv ba^{\varphi(m)-1} \pmod m$.

证明 由于 1, 2, …, m 组成一个模 m 的完全剩余系，又$(a, m) = 1$，故 a, $2a$, …, ma 也组成一个模 m 的完全剩余系. 所以，其中有且仅有一个数设为 aj，满足

$$aj \equiv b \pmod{m},$$

于是 $x \equiv j \pmod{m}$就是式(3.5.2)的唯一解.

因为

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

所以，有

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

即

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

故 $x \equiv a^{\varphi(m)-1} b \pmod{m}$是(3.5.2)式的唯一解.

由定理 3.5.1 可推出，当 $m > 1$, $(a, m) = 1$ 时 $a^{-1} \equiv a^{\varphi(m)-1} \pmod{m}$.

定理 3.5.2 设 $m > 1$, $(a, m) = d > 1$，则同余方程(3.5.2)有解的充要条件是 $d \mid b$. 并且在(3.5.2)式有解时，它的解的个数为 d，且若 $x \equiv x_0 \pmod{m}$是(3.5.2)式的特解，则它的 d 个解为

$$x \equiv x_0 + \frac{m}{d} t \pmod{m},$$

其中 $t = 0, \cdots, d - 1$.

证明 先证必要性. 如果(3.5.2)式有解 $x \equiv x_0 \pmod{m}$，则有

$$m \mid ax_0 - b,$$

又

$$d \mid m,$$

故

$$d \mid ax_0 - b.$$

又因为 $d \mid a$，所以有 $d \mid b$.

再证充分性. 如果 $d \mid b$，则 $\frac{b}{d}$ 为整数，又 $(\frac{a}{d}, \frac{m}{d}) = 1$，根据定理 3.5.1，同余方程

$$\frac{a}{d} x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

有唯一解，由定理 3.1.7，这个解必满足同余方程(3.5.2)式，故(3.5.2)式有解.

若 $x \equiv x_0 \pmod{\frac{m}{d}}$是同余方程

$$\frac{a}{d} x \equiv \frac{b}{d} \pmod{\frac{m}{d}}$$

的唯一解，则有以下 d 个模 m 不同余的整数

$$x_0,\ x_0 + \frac{m}{d},\ x_0 + 2\frac{m}{d},\ \cdots,\ x_0 + (d-1)\frac{m}{d},$$

是(3.5.2)式的解. 由于

$$ax_0 \equiv b \pmod{m},$$

且显然有

$$at\frac{m}{d} \equiv 0 \pmod{m},\ t = 0, \cdots, d - 1,$$

故

$$a(x_0 + t\frac{m}{d}) \equiv b \pmod{m},$$

于是 $x \equiv x_0 + \frac{m}{d}t \pmod m$是(3.5.2)式的解. 又

$$x_0,\ x_0+\frac{m}{d},\ x_0+2\frac{m}{d},\ \cdots,\ x_0+(d-1)\frac{m}{d}$$

两两模 m 不同余，且对于其他解，均可在以上这 d 个解中找到一数与之模 m 同余，即(3.5.2)式只有 d 个解. 证毕.

例 3.5.3 求解一次同余方程 $28x \equiv 21 \pmod{35}$.

解 由于 $d = (28, 35) = 7$，且显然 21 能被 7 整除，故此同余方程有解.

先求出同余方程

$$4x \equiv 3 \pmod 5$$

的解为 $x \equiv 2 \pmod 5$，所以原同余方程

$$28x \equiv 21 \pmod{35}$$

的一个特解为 $x_0 \equiv 2 \pmod{35}$.

于是原同余方程的全部解为

$$x \equiv 2 + 5t \pmod{35},\quad t = 0, 1, \cdots, 4, 5, 6,$$

即 $x \equiv 2, 7, 12, 17, 22, 27, 32 \pmod{35}$.

习题 3.5

A 组

1. 求解下列一次同余方程：
   (1) $27x \equiv 12 \pmod{15}$
   (2) $24x \equiv 6 \pmod{81}$
   (3) $91x \equiv 26 \pmod{169}$
   (4) $71x \equiv 32 \pmod{3441}$
2. 确定下面同余式的不同解的个数，无需求出解.
   (1) $72\ x \equiv 47 \pmod{200}$
   (2) $4183\ x \equiv 5781 \pmod{15087}$
   (3) $1537\ x \equiv 2863 \pmod{6731}$

B 组

1. 编程判断同余方程 $ax \equiv b \pmod m$是否有解，如果有解，求出所有的解.
2. 如果在一个密码系统中，明文 x 被加密成密文 y，使得 $y \equiv 7x+3 \pmod{26}$，那么由密文 y 解密得到明文 x 的公式是什么?

3.6 中国剩余定理与同余方程组

我国古代的一部优秀数学著作《孙子算经》中，有一类叫作“物不知数”的问题，原文如下：

“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？”

这个问题可以表达如下：现有一未知数，被 3 除余 2，被 5 除余 3，被 7 除余 2，求此

未知数. 我国明代数学家程大位(字汝思, 号宾渠, 1533—1606)在《算法统宗》这部著作中, 把解法用一首优美的诗来总结：

三人同行七十稀，五树梅花廿一枝，
七子团圆整半月，除百零五便得知.

这首诗的意思是，将此未知数被 3 除所得的余数乘 70，被 5 除所得的余数乘 21，被 7 除所得的余数乘 15，再将它们求和，将和除以 105，得到的余数即为所求未知数. 于是，以上“物不知数”问题可求解如下：

$$2\times 70 + 3\times 21 + 2\times 15 = 233,$$

将 233 除以 105，余数 23 即为所求.

这个问题为什么可以这样求解？这是不是一种巧合？在这个问题中，我们遇到的是 3 除, 5 除, 7 除，如果用其他的数代替 3, 5, 7，能否有同样类似的解法？著名的“孙子定理”就是用来解决这类问题的.

这其实就是一个求一次同余方程组的问题，此同余方程组表示如下，注意其中每一行的模数各不相同而且两两互素：

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

我们先来直观的看一下这个问题的解法，这个问题看上去是不好解的，但是如果我们换一个类似的问题，就会感觉好解了，如下：

$$\begin{cases} x \equiv 0 \pmod 3 \\ x \equiv 0 \pmod 5 \\ x \equiv 0 \pmod 7 \end{cases}$$

由同余的概念马上可知道，$3|x$，$5|x$，$7|x$，所以 $3\times 5\times 7|x$，即 $105|x$，因此方程组的解必为

$$x \equiv 0 \pmod{105}.$$

让我们再换一个稍微复杂的问题

$$\begin{cases} a \equiv 1 \pmod 3 \\ a \equiv 0 \pmod 5 \\ a \equiv 0 \pmod 7 \end{cases}$$

类似于上面问题的思考思路，由第二和第三式知道 $5\times 7|a$，即 $35|a$，也就是 a 为 35 的倍数，那么接下来要看 35 的倍数中哪些除以 3 余 1，也就是看 35 的倍数中哪些具有如下的性质

$$35\times n \equiv 1 \pmod 3,$$

很明显 35 与 n 互相为模 3 的逆元，35 本身不行，但是 70 就行了（注意这个时候 $n = 2$），从而 70 +105 的倍数也行，所以方程组的解必为

$$a \equiv 70 \pmod{105}.$$

同样的道理，我们对方程组

$$\begin{cases} b \equiv 0 \pmod 3 \\ b \equiv 1 \pmod 5 \\ b \equiv 0 \pmod 7 \end{cases}$$

得到解为

$$b \equiv 21 \pmod{105}.$$

对方程组

$$\begin{cases} c \equiv 0 \pmod 3 \\ c \equiv 0 \pmod 5 \\ c \equiv 1 \pmod 7 \end{cases}$$

得到解为

$$c \equiv 15 \pmod{105}.$$

另外，我们很容易观察到：

$$\begin{cases} 2a \equiv 2 \pmod 3 \\ 2a \equiv 0 \pmod 5 \\ 2a \equiv 0 \pmod 7 \end{cases}$$

$$\begin{cases} 3b \equiv 0 \pmod 3 \\ 3b \equiv 3 \pmod 5 \\ 3b \equiv 0 \pmod 7 \end{cases}$$

和

$$\begin{cases} 2c \equiv 0 \pmod 3 \\ 2c \equiv 0 \pmod 5 \\ 2c \equiv 2 \pmod 7 \end{cases}$$

所以，原来方程的解必为

$$x \equiv 2a + 3b + 2c \pmod{105}.$$

前面提及的实际数值解答为

$$x \equiv 2\times 70 + 3\times 21 + 2\times 15 = 233 \equiv 23 \pmod{105}.$$

将此问题推广，我们可给出下面定理.

定理 3.6.1 设 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数，若令

$$m = m_1 m_2 \cdots m_k, \quad M_{i=} m_1 m_2 \ldots m_{i-1} m_{i+1} \ldots m_k, m = m_i M_i, \quad i = 1, 2, \cdots, k,$$

则对任意的整数 $b_1, \cdots, b_k$，同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \quad\vdots \\ x \equiv b_k \pmod{m_k} \end{cases} \tag{3.6.1}$$

有唯一解

$$x \equiv M_1' M_1 b_1 + M_2' M_2 b_2 + \cdots + M_k' M_k b_k \pmod m, \tag{3.6.2}$$

其中

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

证明 由于对任意给定的 i 和 j，若满足 $1 \leqslant i, j \leqslant k$ 且 $i \neq j$，则有

$$(m_i, m_j) = 1,$$

故

$$(m_i, M_i) = 1.$$

于是对每一个 M_i，存在一个唯一的 M_i'，$i = 1, 2, \cdots, k$，使得

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

又由 $m = m_i M_i$，得 $m_i \mid M_j$，$i \neq j$，因此

$$M_1' M_1 b_1 + M_2' M_2 b_2 + \cdots + M_k' M_k b_k \equiv M_i' M_i b_i \equiv b_i \pmod{m_i}, \quad i = 1, 2, \cdots, k,$$

即(3.6.2)式是同余方程组(3.6.1)的解.

再证明这个解的唯一性. 设 x_1, x_2 是满足同余方程组(3.6.1)的任意两个整数，则

$$x_1 \equiv x_2 \equiv b_i \pmod{m_i}, \quad i = 1, 2, \cdots, k.$$

因为 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数，进而有

$$x_1 \equiv x_2 \pmod{m},$$

即解是唯一的.

这个定理就是著名的**中国剩余定理**.

例 3.6.1 求解同余方程组

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 4 \pmod 7 \\ x \equiv 6 \pmod{13} \end{cases}$$

解 利用定理 3.6.1，其中 $m_1 = 3$，$m_2 = 5$，$m_3 = 7$，$m_4 = 13$. 令 $m = m_1 m_2 m_3 m_4 = 1\,365$，则

$$M_1 = m_2 m_3 m_4 = 455, \quad M_2 = m_1 m_3 m_4 = 273,$$
$$M_3 = m_1 m_2 m_4 = 195, \quad M_4 = m_1 m_2 m_3 = 105,$$

分别求解同余方程

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

得

$$M_1' = 2, \quad M_2' = 2, \quad M_3' = 6, \quad M_4' = 1,$$

故此同余方程组的解为

$$x \equiv 2 \times 455 \times 1 + 2 \times 273 \times 2 + 6 \times 195 \times 4 + 1 \times 105 \times 6 \equiv 7\,312 \equiv 487 \pmod{1\,365}.$$

定理 3.6.2 设 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数，令

$$m = m_1 m_2 \cdots m_k,$$
$$m = m_i M_i,$$
$$M_i' M_i \equiv 1 \pmod{m_i}, \quad i = 1, 2, \cdots, k,$$

若 $b_1, b_2, \cdots, b_k$ 分别遍历模 $m_1, m_2, \cdots, m_k$ 的完全剩余系，则

$$M_1' M_1 b_1 + M_2' M_2 b_2 + \cdots + M_k' M_k b_k$$

遍历模 m 的完全剩余系.

证明 令

$$x_0 = M_1' M_1 b_1 + M_2' M_2 b_2 + \cdots + M_k' M_k b_k \pmod m,$$

则当 $b_1, b_2, \cdots, b_k$ 分别遍历模 $m_1, m_2, \cdots, m_k$ 的完全剩余系时，x_0 遍历 m 个整数. 下面证明这 m 个整数两两模 m 不同余. 若

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

其中 b_i 和 b_i' 在同一个模 m_i 的完全剩余系中取值，由于 $m_i \mid m$，$m_i \mid M_j$，$i \neq j$，故

$$M_i' M_i b_i \equiv M_i' M_i b_i' \pmod{m_i}, \quad i = 1, 2, \cdots, k,$$

又因为

$$M_i' M_i \equiv 1 \pmod{m_i}, \quad i = 1, 2, \cdots, k,$$

所以

$$b_i \equiv b_i' \pmod{m_i},\quad i = 1, 2, \cdots, k.$$

由于 b_i 和 b_i' 在同一个模 m_i 的完全剩余系中取值，故只能有

$$b_i = b_i',\quad i = 1, 2, \cdots, k.$$

定理得证.

以上定理可以看作是定理 3.2.4 的推广.

定理 3.6.3 同余方程组

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

有解的充要条件是$(m_1, m_2) \mid (b_1 - b_2)$. 如果上述条件成立，则同余方程组模$[m_1, m_2]$有唯一解.

证明 设$(m_1, m_2) = d$，先证必要性. 若 x_0 为同余方程组的解，则有

$$x_0 \equiv b_1 \pmod{d},\qquad x_0 \equiv b_2 \pmod{d},$$

两式相减得 $b_1 - b_2 \equiv 0 \pmod{d}$，因此 $d \mid b_1 - b_2$.

再证充分性. 若 $d \mid b_1 - b_2$，则因 $x \equiv b_1 \pmod{m_1}$的解可写为

$$x = b_1 + m_1 y,$$

将其代入 $x \equiv b_2 \pmod{m_2}$得

$$m_1 y \equiv b_2 - b_1 \pmod{m_2}.$$

因为$(m_1, m_2) = d$，$d \mid b_2 - b_1$，故上式有解，即原同余方程组有解.

设原同余方程组有两个解分别为 x_1 和 x_2，则

$$x_1 - x_2 \equiv 0 \pmod{m_1},\qquad x_1 - x_2 \equiv 0 \pmod{m_2},$$

于是有 $x_1 - x_2 \equiv 0 \pmod{[m_1, m_2]}$，即同余方程组模$[m_1, m_2]$有唯一解. 证毕.

通过以上述定理可知，对于一次同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \quad\vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

其中 $k \geqslant 3$，若$(m_1, m_2) \mid b_1 - b_2$，可先解前面两个方程得

$$x \equiv b_2' \pmod{[m_1, m_2]}.$$

若$([m_1, m_2], m_3) \mid b_2' - b_3$，则可再与后面的 $x \equiv b_3 \pmod{m_3}$联立解出

$$x \equiv b_3' \pmod{[m_1, m_2, m_3]}.$$

依此类推，最后可得唯一解

$$x \equiv b_k' \pmod{[m_1, m_2, \cdots, m_k]}.$$

如果中间有一步出现无解，则原同余方程组无解.

例 3.6.2 判断方程组

$$\begin{cases} x \equiv 11 \pmod{36} \\ x \equiv 7 \pmod{40} \\ x \equiv 32 \pmod{75} \end{cases}$$

是否有解.

解 $(36, 40) = 4$，$(36, 75) = 3$，$(40, 75) = 5$.

$b_1 - b_2 = 11 - 7 = 4$,

$b_1 - b_3 = 1 - 32 = -21$,

$$b_2 - b_3 = 7 - 32 = -25.$$

因此方程组肯定有解，因为方程组满足有解条件，即 $4 \mid 4$，$3 \mid -21$，$5 \mid -25$. 且解的模数是 $[36, 40, 75] = 1\,800$. 这个方程的解为 $x \equiv 407 \pmod{1\,800}$. 有兴趣的读者可以自行练习写出全部求解过程.

定理 3.6.4 设 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数，令 $m = m_1 m_2 \cdots m_k$，则同余方程

$$f(x) \equiv 0 \pmod{m} \tag{3.6.3}$$

与同余方程组

$$\begin{cases} f(x) \equiv 0 \pmod{m_1} \\ f(x) \equiv 0 \pmod{m_2} \\ \quad\vdots \\ f(x) \equiv 0 \pmod{m_k} \end{cases} \tag{3.6.4}$$

等价. 若用 T_i 表示同余方程

$$f(x) \equiv 0 \pmod{m_i}$$

的解数（即解的个数），$i = 1, 2, \cdots, k$，用 T 表示同余方程(3.6.3)的解数，则

$$T = T_1 T_2 \cdots T_k.$$

证明 设 x_0 为同余方程(3.6.3)的解，则

$$f(x_0) \equiv 0 \pmod{m}.$$

由定理 3.1.8 可知

$$f(x_0) \equiv 0 \pmod{m_i}, \quad i = 1, 2, \cdots, k,$$

即 x_0 亦为同余方程组(3.6.4)的解.

若 x_0 为同余方程组(3.6.4)的解，即

$$f(x_0) \equiv 0 \pmod{m_i}, \quad i = 1, 2, \cdots, k.$$

由定理 3.1.9 可知

$$f(x_0) \equiv 0 \pmod{m},$$

即 x_0 亦为同余方程(3.6.3)的解.

设同余方程 $f(x) \equiv 0 \pmod{m_i}$的解为 b_i，$i = 1, 2, \cdots, k$. 由孙子定理可知同余方程组

$$\begin{cases} x \equiv b_1 \pmod{m_1} \\ x \equiv b_2 \pmod{m_2} \\ \quad\vdots \\ x \equiv b_k \pmod{m_k} \end{cases}$$

的解为

$$x \equiv M_1' M_1 b_1 + M_2' M_2 b_2 + \cdots + M_k' M_k b_k \pmod{m}.$$

由于

$$f(x) \equiv f(b_i) \equiv 0 \pmod{m_i}, \quad i = 1, 2, \cdots, k,$$

故 x 亦为同余方程(3.6.3)的解. 于是当 b_i 遍历 $f(x) \equiv 0 \pmod{m_i}$的所有解时，x 遍历同余方程(3.6.3)的所有解. 于是，有 $T = T_1 T_2 \cdots T_k$.

例 3.6.3 求解同余方程

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

解 设 $f(x) = x^4 + 2x^3 + 8x + 9$，由定理 3.6.4 知同余方程 $f(x) \equiv 0 \pmod{35}$等价于同余方程组

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

用直接验算的方法容易得到 $f(x) \equiv 0 \pmod 5$ 的解为

$$x \equiv 1, 4 \pmod 5,$$

$f(x) \equiv 0 \pmod 7$ 的解为

$$x \equiv 3, 5, 6 \pmod 7.$$

由孙子定理，可求出同余方程组

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

当 (b_1, b_2) 分别取 $(1, 3)$，$(1, 5)$，$(1, 6)$，$(4, 3)$，$(4, 5)$，$(4, 6)$ 时的解为

$$x \equiv 21b_1 + 15b_2 \equiv 31, 26, 6, 24, 19, 34 \pmod{35}.$$

这 6 个解即为原同余方程的解.

这个定理使我们能够利用孙子定理来解单个的具有较大模数的线性同余方程，这种方法可能在计算上更有效率.

例 3.6.4 求解 $13x \equiv 71 \pmod{380}$.

解 因为 $380 = 4 \times 5 \times 19$，所以它等价于如下方程组

$$\begin{cases} 13x \equiv 71 \pmod 4 \\ 13x \equiv 71 \pmod 5 \\ 13x \equiv 71 \pmod{19} \end{cases}$$

$$\Rightarrow \begin{cases} (4+4+4+1)x \equiv 71 \pmod 4 \\ (5+5+3)x \equiv 71 \pmod 5 \\ 13x \equiv 71 \pmod{19} \end{cases}$$

$$\Rightarrow \begin{cases} x \equiv 71 \pmod 4 \\ 3x \equiv 71 \pmod 5 \\ 13x \equiv 71 \pmod{19} \end{cases}$$

$$\Rightarrow \begin{cases} x \equiv 3 \pmod 4 \\ 3x \equiv 1 \pmod 5 \\ 13x \equiv 14 \pmod{19} \end{cases}$$

利用单同余方程式的解法可得到

$$\begin{cases} x \equiv 3 \pmod 4 \\ x \equiv 2 \pmod 5 \\ x \equiv 4 \pmod{19} \end{cases}$$

接着应用孙子定理求解即可，最后得到的解为

$$x \equiv 327 \pmod{380}.$$

前面讨论的同余方程组问题中，我们注意到方程组中的每一行的模数都不相同，而且只有一个待解的未知元. 还有另一类重要的多元线性同余方程组问题，不同之处在于这类问题中的模数都相同，而且具有两个或者两个以上的未知元. 这样的问题与我们在线性代

数中学过的关于实数和复数的方程组问题非常相像，而且可以使用很多线性代数中的向量和矩阵的表示及运算方法．下面通过实例来加深读者对此的理解．

例 3.6.5　在古典的 Hill 密码中，如果按对加密，则每一对明文组成的行向量用(x_1, x_2)来表示，加密后的密文对形成的行向量用(y_1, y_2)来表示，y_1, y_2 是由 x_1, x_2 的线性组合计算而来

$$\begin{cases} y_1 \equiv 11x_1 + 3x_2 \pmod{26} \\ y_2 \equiv 8x_1 + 7x_2 \pmod{26} \end{cases}$$

使用矩阵表达即为

$$(y_1, y_2) \equiv (x_1, x_2)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} \pmod{26}.$$

其中的 2 乘 2 阶矩阵被称作密钥，那么如何解密呢，即如何由(y_1, y_2)来计算得到(x_1, x_2)呢？实际上，我们可以采用消元方法来解，先消去未知元 x_2 解得 x_1，然后同样的方法，先消去未知元 x_1 解得 x_2．还可以利用逆矩阵的方法，即

$$(x_1, x_2) \equiv (y_1, y_2)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}^{-1} (\mathrm{mod}\, 26),$$

其中

$$\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}.$$

我们可以验证一下这个逆矩阵的正确性：

$$\begin{aligned} &\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} \\ =&\begin{pmatrix} 11\times 7 + 8\times 23 & 11\times 18 + 8\times 11 \\ 3\times 7 + 7\times 23 & 3\times 18 + 7\times 11 \end{pmatrix} \\ =&\begin{pmatrix} 261 & 286 \\ 182 & 131 \end{pmatrix} \\ \equiv&\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} (\mathrm{mod}\, 26) \end{aligned}$$

两者的乘积是单位矩阵，说明它们互为逆矩阵．

如果明文是$(x_1, x_2) = (9, 20)$，计算过程如下：

$$(9, 20)\begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix} = (99 + 60, 72 + 140) \equiv (3, 4) (\mathrm{mod}\, 26).$$

则密文为(3, 4)．反过来，接收方收到密文(3, 4)后，希望恢复明文，计算过程如下：

$$(3, 4)\begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix} = (21 + 92, 54 + 44) \equiv (9, 20) \pmod{26},$$

可见的确正确地恢复了明文(9, 20).

那么，在模 26 运算下，如何判断矩阵是否可逆？又如何计算可逆矩阵的逆矩阵呢？下面我们不加证明地给出有关定理．

定理 3.6.5　矩阵 **K** 在模 26 运算下存在可逆矩阵的充分必要条件是(det **K**, **26**) = 1 (det **K** 表示矩阵 **K** 的行列式的值).

定理 3.6.6　如果二阶矩阵

$$K=\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}$$

可逆，则其逆矩阵为

$$K^{-1}=(\det K)^{-1}\begin{pmatrix} k_{22} & -k_{12} \\ -k_{21} & k_{11} \end{pmatrix} \pmod{26}.$$

习题 3.6

A 组

1. 求解同余方程组.

(1) $\begin{cases} x\equiv 9 \pmod{12} \\ x\equiv 6 \pmod{25} \end{cases}$　　(2) $\begin{cases} x\equiv 5 \pmod{7} \\ x\equiv 12 \pmod{15} \\ x\equiv 18 \pmod{22} \end{cases}$

(3) $\begin{cases} x\equiv 2 \pmod{9} \\ 3x\equiv 4 \pmod{5} \\ 4x\equiv 3 \pmod{7} \end{cases}$

2. 求解下列同余方程组（注意不只一个解）：

$$\begin{cases} 2x\equiv 3 \pmod{5} \\ 4x\equiv 2 \pmod{6} \\ 3x\equiv 2 \pmod{7} \end{cases}$$

3. 有总数不满 50 人的一队士兵，一至三报数，最后一人报“一”；一至五报数，最后一人报“二”；一至七报数，最后一人也报“二”. 这队士兵有多少人？

4. 利用转化成联立方程组的方法解 $91x\equiv 419 \pmod{440}$.

B 组

1. 求 13 的倍数，使得该数被 3, 5, 7, 11 除所得的余数均为 2.

2. 求相邻的 4 个正整数，它们依次可被 2^2, 3^2, 5^2 及 7^2 整除.

3. 编程实现中国剩余定理.

4. 已知 Hill 密码中的明文分组长度是 2，密钥 $\boldsymbol{K}$ 是一个 2 阶可逆方阵. 假设明文 3, 14, 2, 19 所对应的密文是 1, 14, 11, 21，试求密钥 $\boldsymbol{K}$.

3.7* 高次同余方程

我们知道，任一大于 1 的整数 m 均有标准分解式：

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \quad \alpha_i > 0, \quad i = 1, 2, \cdots, s,$$

其中 $p_i < p_j$（$i < j$）是素数. 于是，由定理 3.6.4 可知，欲解 $f(x) \equiv 0 \pmod m$，只需求解同余方程组

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

所以，我们先来讨论 p 为素数时，同余方程

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod{p^\alpha} \tag{3.7.1}$$

的求解方法，其中 α 为正整数，且 a_n 不能被 p^α 整除.

定理 3.7.1 设 $x \equiv x_1 \pmod p$是同余方程

$$f(x) \equiv 0 \pmod p \tag{3.7.2}$$

的一个解，且满足($f'(x_1)$, p) = 1，则同余方程(3.7.1)有解

$$x \equiv x_\alpha \pmod{p^\alpha}.$$

其中 x_α 由以下关系式递归得到：

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

$i = 2, 3, \cdots, \alpha$. 这里，$f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$ 表示 $f(x)$的导函数.

证明 用数学归纳法.

(1) 当 $\alpha = 2$ 时，根据假设条件，同余方程(3.7.2)的所有解为

$$x = x_1 + p t_1, \quad t_1 = 0, \pm 1, \pm 2, \cdots.$$

于是，我们考虑关于 t_1 的同余方程

$$f(x_1 + p t_1) \equiv 0 \pmod{p^2}.$$

由泰勒公式，有

$$f(x_1) + p t_1 f'(x_1) \equiv 0 \pmod{p^2},$$

又因为 $f(x_1) \equiv 0 \pmod p$，所以上述同余方程可写为

$$t_1 f'(x_1) \equiv -\frac{f(x_1)}{p} \pmod p .$$

由($f'(x_1)$, p) = 1，根据定理 3.5.2，此同余方程的唯一解为

$$t_1 \equiv -\frac{f(x_1)}{p} \left((f'(x_1))^{-1} \pmod p \right) \pmod p \quad .$$

故

$$x \equiv x_2 \equiv x_1 + p t_1 \pmod{p^2}$$

是同余方程 $f(x) \equiv 0 \pmod{p^2}$的解.

(2) 当 $\alpha \geqslant 3$ 时，假设对 $i-1$ $(3 \leqslant i \leqslant \alpha)$ 成立，即同余方程

$$f(x) \equiv 0 \pmod{p^{i-1}}$$

有解

$$x = x_{i-1} + p^{i-1}t_{i-1},\ \ t_{i-1} = 0,\ \pm 1,\ \pm 2,\ \cdots.$$

于是，我们考虑关于t_{i-1}的同余方程

$$f(x_{i-1} + p^{i-1}t_{i-1}) \equiv 0 \pmod{p^i}.$$

由泰勒公式及$p^{2(i-1)} \geqslant p^i$，可知

$$f(x_{i-1}) + p^{i-1}t_{i-1}f'(x_{i-1}) \equiv 0 \pmod{p^i},$$

因为$f(x_{i-1}) \equiv 0 \pmod{p^{i-1}}$，所以上述同余方程可写为

$$t_{i-1}f'(x_{i-1}) \equiv -\frac{f(x_{i-1})}{p^{i-1}} \pmod{p}.$$

又$f'(x_{i-1}) \equiv f'(x_{i-2}) \equiv \cdots \equiv f'(x_1) \pmod{p}$，进而有

$$(f'(x_{i-1}), p) = \cdots = (f'(x_1), p) = 1,$$

再根据定理 3.5.2，此同余方程的唯一解为

$$\begin{aligned} t_{i-1} &\equiv -\frac{f(x_{i-1})}{p^{i-1}}\left((f'(x_{i-1}))^{-1} \pmod{p}\right) \\ &\equiv -\frac{f(x_{i-1})}{p^{i-1}}\left((f'(x_1))^{-1} \pmod{p}\right) \pmod{p} \end{aligned}$$

故

$$x \equiv x_i \equiv x_{i-1} + p^{i-1}t_{i-1} \pmod{p^i}$$

是同余方程$f(x) \equiv 0 \pmod{p^i}$的解.

于是，根据数学归纳法，定理得证.

例 3.7.1 求解同余方程

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

解 写出$f(x)$的导函数，即

$$f'(x) = 4x^3 + 7.$$

通过直接验算，可知同余方程

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

有一解

$$x_1 \equiv 1 \pmod{3}.$$

于是，有

$$f'(x_1) \equiv -1 \pmod{3},$$

进而

$$\left(f'(x_1)\right)^{-1} \equiv -1 \pmod{3}.$$

依次计算如下:

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

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

所以，原同余方程的解为

$$x_3 \equiv 22 \pmod{27}.$$

现在我们重点讨论模 p 的同余方程

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \equiv 0 \pmod p \tag{3.7.3}$$

的求解方法，其中 a_n 不能被 p 整除.

在此之前，我们先引入多项式的辗转相除法，或称多项式的欧几里得除法.

定理 3.7.2 设

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0$$

为 n 次整系数多项式,

$$g(x) = x^m + b_{m-1}x^{n-1} + \cdots + b_1 x + b_0$$

为 m 次首一（最高项系数为 1）整系数多项式，其中 $m \geqslant 1$，则存在整系数多项式 $q(x)$和 $r(x)$使得

$$f(x) = g(x)q(x) + r(x),$$

其中 $\deg r(x) < \deg g(x)$.

证明 我们可分两种情况讨论.

(1) 若 $n < m$，可取 $q(x) = 0$，$r(x) = f(x)$使结论成立.

(2) 若 $n \geqslant m$，可对 $f(x)$的次数 n 作数学归纳法.

当 $n = m$ 时，有

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

因此，取 $q(x) = a_n$，$r(x) = f(x) - a_n g(x)$可使结论成立.

假设当 $n = k - 1$ 时，结论成立，其中 $k - 1 \geqslant m$.

当 $n = k$ 时，则有

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

显然 $f(x) - a_n x^{n-m} g(x)$是次数小于等于 $n-1$ 的多项式，对其运用归纳假设或情况(1)，可知存在整系数多项式 $q_1(x)$和 $r_1(x)$使得

$$f(x) - a_n x^{n-\mathrm{m}} g(x) = g(x)q_1(x) + r_1(x),$$

其中 $\deg r_1(x) < \deg g(x)$. 因此，取 $q(x) = a_n x^{n-\mathrm{m}} + q_1(x)$，$r(x) = r_1(x)$可使结论成立.

根据数学归纳法原理，可知结论成立，于是定理得证.

定理 3.7.3 同余方程(3.7.3)与一个次数小于 p 的模 p 的同余方程等价.

证明 由定理 3.7.2 可知，存在整系数多项式 $q(x)$和 $r(x)$使得

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

其中 $\deg r(x) < p$. 根据费马小定理，对任意整数 x 都有

$$x^p - x \equiv 0 \pmod p.$$

于是同余方程

$$f(x) \equiv 0 \pmod p$$

等价于同余方程

$$r(x) \equiv 0 \pmod p.$$

定理 3.7.4 同余方程(3.7.3)最多有 n 个解.

证明 可对 $f(x)$的次数 n 作数学归纳法.

当 $n = 1$ 时，一次同余方程为

$$a_1x + a_0 \equiv 0 \pmod{p},$$

由于 a_1 不能被 p 整除，即$(a_1, p) = 1$，故同余方程恰有一个解，结论成立.

假设定理对次数为 $n-1$ $(n\geqslant 2)$的同余方程成立，即次数为 $n-1$ 的同余方程最多有 $n-1$ 个解. 下面证明同余方程(3.7.3)最多有 n 个解.

根据定理 3.7.3 可知，同余方程(3.7.3)与一个次数小于 p 的模 p 的同余方程等价，所以不妨设 $n\leqslant p-1$. 用反证法，假设同余方程(3.7.3) 有 $n+1$ 个解，设它们为

$$x \equiv x_i \pmod{p},\quad i = 0, 1, \cdots, n.$$

由于

$$f(x) - f(x_0) = \sum_{k=1}^{n} a_k (x^k - x_0^k) = (x - x_0)g(x),$$

显然，$g(x)$是首项系数为 a_n 的 $n-1$ 次整系数多项式，根据归纳假设，可知

$$g(x) \equiv 0 \pmod{p}$$

是 $n-1$ 次同余方程，至多有 $n-1$ 个解. 而由于

$$f(x_k) - f(x_0) = (x_k - x_0)g(x_k) \equiv 0 \pmod{p}$$

当 $k>0$ 时，$x_k - x_0 \equiv 0 \pmod{p}$不成立，故 $n-1$ 次同余方程 $g(x) \equiv 0 \pmod{p}$有 n 个解，推出了矛盾. 于是假设不成立，定理得证.

定理 3.7.4 通常被称为**拉格朗日(Lagrange)定理**.

定理 3.7.5 如果同余方程

$$f(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0 \equiv 0 \pmod{p}$$

的解的个数大于 n，则 $p \mid a_i$，$i = 0, 1, \cdots, n$.

证明 用反证法. 假设存在某些系数不能被 p 整除，若这些系数的下标最大的为 k，$k \leqslant n$，则原同余方程可写为

$$f(x) \equiv a_kx^k + a_{k-1}x^{k-1} + \cdots + a_1x + a_0 \equiv 0 \pmod{p}.$$

根据上面的定理可知，此同余方程最多有 k 个解，与所给条件矛盾，故假设不成立. 定理得证.

定理 3.7.6 如果同余方程(3.7.3)有 k 个不同的解

$$x \equiv x_i \pmod{p},\quad i = 1, 2, \cdots, k,\ 1\leqslant k\leqslant n,$$

则对任意整数 x，均有

$$f(x) \equiv (x - x_1)(x - x_2)\cdots(x - x_k)f_k(x) \pmod{p},$$

其中 $f_k(x)$是首项系数为 a_n 的 $n-k$ 次多项式.

证明 由定理 3.7.2 可知，存在整系数多项式 $f_1(x)$和 $r(x)$使得

$$f(x) = (x - x_1)f_1(x) + r(x),\quad \deg r(x) < \deg (x - x_1).$$

显然，$f_1(x)$是首项系数为 a_n 的 $n-1$ 次多项式. 由于 $\deg (x - x_1) = 1$，故 $r(x) = r$ 为整数，又因为 $f(x_1) \equiv 0 \pmod{p}$，所以有 $r \equiv 0 \pmod{p}$，即

$$f(x) = (x - x_1)f_1(x) \pmod{p}.$$

又因为 $f(x_i) \equiv 0 \pmod{p}$，并且 x_i 与 x_1 模 p 不同余，其中 $i = 2, 3, \cdots, k$，于是可知

$$f_1(x_i) \equiv 0 \pmod{p},\ i = 2, 3, \cdots, k.$$

同理，对多项式 $f_1(x)$可找到多项式 $f_2(x)$使得

$$\begin{cases} f_1(x) \equiv (x - x_2)f_2(x) & (\bmod\ p) \\ f_2(x_i) \equiv 0 & (\bmod\ p) \end{cases}$$

其中 $i = 3, 4, \cdots, k$. 依此类推，可得

$$f_{k-1}(x) \equiv (x - x_k)f_k(x) \pmod{p}.$$

于是，有

$$f(x)\equiv(x-x_1)\cdots(x-x_k)\,f_k(x)\pmod p,$$

定理得证.

定理 3.7.7 对于素数 p 与正整数 n，$n\leqslant p$，同余方程

$$f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\equiv 0\pmod p$$

有 n 个解的充要条件是 x^p-x 被 $f(x)$除所得余式的所有系数均能被 p 整除.

证明 由定理 3.7.2 可知，存在整系数多项式 $q(x)$和 $r(x)$，使得

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

其中 $r(x)$的次数小于 n，$q(x)$的次数为 $p-n$.

现在证明必要性. 若原同余方程有 n 个解，则根据费马小定理，这 n 个解都是

$$x^p-x\equiv 0\pmod p$$

的解，显然这 n 个解也都是

$$r(x)\equiv 0\pmod p$$

的解. 由于 $r(x)$的次数小于 n，故由定理 3.7.5 可知，$r(x)$的所有系数均能被 p 整除.

再来证明充分性. 若 $r(x)$的所有系数均能被 p 整除，则显然有

$$r(x)\equiv 0\pmod p.$$

又由费马小定理，可知对任意整数有

$$x^p-x\equiv 0\pmod p.$$

因此，对任意整数有

$$f(x)q(x)\equiv 0\pmod p,$$

即它有 p 个不同的解

$$x\equiv 0,\,1,\,\cdots,\,p-1\pmod p.$$

假设 $f(x)\equiv 0\pmod p$的解数小于 n，则 $q(x)\equiv 0\pmod p$的解数小于等于 $p-n$，故

$$f(x)q(x)\equiv 0\pmod p$$

的解数小于 p，推出了矛盾. 所以 $f(x)\equiv 0\pmod p$的解数为 n. 证毕.

例 3.7.2 判断同余方程

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

解的个数.

解 先将多项式化为首项系数为 1. 由于 $4\times 2\equiv 1\pmod 7$，故我们有

$$4(2x^3+5x^2+6x+1)\equiv x^3-x^2+3x-3\equiv 0\pmod 7.$$

根据多项式的辗转相除法，可得

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

由上面定理可知原同余方程有 3 个解.

习题 3.7

A 组

1. 求解同余方程

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

   (2) $x^3+5x^2+9\equiv 0\pmod{27}$.

2. 证明同余方程

$$2x^3-x^2+3x+11\equiv 0\pmod 5$$

有 3 个解.

4. 如下各个方程有几个解？

$x^2-1\equiv 0 \pmod{168}$；

$x^2+1\equiv 0 \pmod{70}$；

$x^2+x+1\equiv 0 \pmod{91}$；

$x^3+1\equiv 0 \pmod{140}$.

B 组

1. 举例说明对模数为合数的情况，拉格朗日定理一般不成立.