第 2 章　同余

同余是数论中极为重要的另一个概念, 在后面的第 5 和第 6 章中也会提及, 如陪集和商群等概念. 同余理论在密码学，特别是公钥密码学中有着非常重要的应用. 本章我们主要介绍同余、同余关系、剩余类、完全剩余系和缩剩余系等基本概念和性质. 另外, 我们还将讨论欧拉定理、费马小定理、利用扩展欧几里得算法进行快速模逆运算和威尔逊定理等.

学习本章之后，我们应该能够

- 掌握同余的概念与性质，以及相关的计算方法；
- 掌握剩余类和剩余系的概念与性质，以及相关的计算方法；
- 掌握欧拉定理和费马小定理及其相关的应用；
- 掌握扩展欧几里德算法和威尔逊定理及其相关的应用.

2.1　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 $2|(a-b)$, 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 2.1.1　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

$$a \equiv b \pmod{m}; \tag{2.1.1}$$

否则, 称 a 和 b 模 m **不同余**, 记作

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

关系式(2.1.1)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 2.1.1　整数 a 和 b 模 m 同余的充要条件是 $m|a-b$.

证明　先证必要性. 由 $a \equiv b \pmod m$, 可设

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

则 $a - b = m(q_1 - q_2)$, 即 $m|a-b$.

再证充分性. 设

$$a = mq_1 + r_1,\ 0 \leqslant r_1 < m,$$

$$b = mq_2 + r_2,\ 0 \leqslant r_2 < m,$$

则 $a - b = m(q_1 - q_2) + r_1 - r_2$. 由 $m|a-b$, 可知 $m|\ r_1 - r_2$, 则 $m||r_1 - r_2|$. 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$|r_1-r_2|<m$, 故$|r_1-r_2|=0$, 所以$r_1=r_2$. 定理得证.

□

于是, 由定理 2.1.1，同余又可以定义如下, 即若$m|a-b$, 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 2.1.2 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. 等价关系是 2.2 节“剩余类和剩余系”的基础. 有关**等价关系**的概念和性质，请参见 5.1 节“映射与关系”.

定理 2.1.3 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$m|a-b$和$m|b-c$, 得到$m|[(a-b)+(b-c)]$, 即$m|a-c$.

□

定理 2.1.4 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$m|a_1-b_1$, $m|a_2-b_2$, 故$m|x(a_1-b_1)+y(a_2-b_2)$, 又

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

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

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

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

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

(3) 由(2)可证.

□

例 2.1.1 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

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

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 2.1.2 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

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

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

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

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 2.1.5 设 $f(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$ 与 $g(t) = b_n t^n + b_{n-1} t^{n-1} + \cdots + b_1 t + b_0$ 是两个整系数多项式, 满足

$$a_i \equiv b_i \pmod{m}, \qquad 0 \leqslant i \leqslant n,$$

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

$$x^i \equiv y^i \pmod{m}, \qquad 0 \leqslant i \leqslant n,$$

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

$$a_i x^i \equiv b_i y^i \pmod{m},\ 0 \leqslant i \leqslant n,$$

将这些同余式左右对应相加, 可得

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \equiv b_n y^n + b_{n-1} y^{n-1} + \cdots + b_1 y + b_0 \pmod{m},$$

即 $f(x) \equiv g(y) \pmod{m}$.

□

例 2.1.3 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:

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

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

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

命题得证.

□

例 2.1.4 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. 命题得证.

□

定理 2.1.6 若 $ac \equiv bc \pmod m$, 且$(c, m) = d$, 则 $a \equiv b \pmod{\frac{m}{d}}$.

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

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

定理得证.

□

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

定理 2.1.7 若 $a \equiv b \pmod m$, 则有 $ak \equiv bk \pmod{mk}$, 其中 k 为正整数.

证明 由 $m | a - b$, 可知 $mk | ak - bk$, 即 $ak \equiv bk \pmod{mk}$. 定理得证.

□

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

定理 2.1.8 若 $a \equiv b \pmod m$, 且有正整数 d 满足 $d | m$, 则 $a \equiv b \pmod d$.

证明 由 $m | a - b$, $d | m$, 可知 $d | a - b$, 即 $a \equiv b \pmod d$. 定理得证.

□

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

定理 2.1.9 若 $a \equiv b \pmod{m_i}$, $i = 1, 2, \ldots, n$, 则

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

证明 由 $m_i | a - b$, $i = 1,2,\ldots,n$, 可知$[m_1,m_2,\ldots,m_n] | a - b$, 即 $a \equiv b \pmod{[m_1, m_2,\ldots,m_n]}$. 定理得证.

□

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 2.1.10 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 2.1

A 组

1. 证明以下同余式成立：

   (1) $13 \equiv 1 \pmod 2$;　　(2) $91 \equiv 0 \pmod{13}$;

   (3) $-2 \equiv 1 \pmod 3$;　　(4) $111 \equiv -9 \pmod{40}$.

2. 以下同余式对哪些正整数 m 成立：

   (1) $28 \equiv 6 \pmod m$;　　(2) $632 \equiv 2 \pmod m$;

   (3) $73 \equiv 3 \pmod m$;　　(4) $1\ 331 \equiv 0 \pmod m$.

3. (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.

4. 已知 2021 年 10 月 1 日是星期五, 问之后第 2^{280} 天是星期几？

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

6. 证明如果 $m(m > 2)$是整数，则$(a+b) \bmod m \equiv ((a \bmod m)+(b \bmod m)) \bmod m$, 对于所有整数 a 和 b 都成立.

7. 证明如果 $m(m > 2)$是整数，则$(ab) \bmod m \equiv ((a \bmod m)(b \bmod m)) \bmod m$, 对于所有整数 a 和 b 都成立.

8. 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.

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

10. 设 A=$\{d_1, d_2, \ldots, d_k\}$为非零整数 a 的全体因数的集合，证明 B=$\{a/d_1, a/d_2, \ldots, a/d_k\}$ 也是 a 的全体因数的集合.

B 组

11. 计算 555^{555} 被 7 除的余数.

12. 证明如果 a 是奇数，则 $a^2 \equiv 1 \pmod 8$.

13. 证明如果 a、b 和 m 是整数, 且 $m > 0$, $a \bmod m \equiv b \bmod m$，则 $a \equiv b \pmod m$.

14. 证明如果 n 是正奇整数，则

$$1 + 2 + 3 + \cdots + n \equiv 0 \pmod n.$$

   如果 n 是正偶整数，此陈述仍然成立吗？

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

16. 证明如果 $a_j \equiv b_j \pmod m$ $(j = 1, 2, \ldots, n)$，其中 m 是一个正整数， a_j, b_j $(j = 1, 2, \ldots, n)$是

整数，则

(1) $\sum_{j=1}^{n} a_j \equiv \sum_{j=1}^{n} b_j \pmod{m}$.

(2) $\prod_{j=1}^{n} a_j \equiv \prod_{j=1}^{n} b_j \pmod{m}$.

2.2 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 2.2.1 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整数叫作该类的**代表元**.

我们可以用集合的形式来描述剩余类的定义, 即

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

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 2.2.1 设 m 为一正整数, $C_0, C_1, \ldots, C_{m-1}$ 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 $C_0, C_1, \ldots, C_{m-1}$ 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,

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

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

定义 2.2.2 在模 m 的剩余类 $C_0, C_1, \ldots, C_{m-1}$ 中各取一代表元 $a_i\in C_i$, $i = 0, 1, \ldots, m-1$, 则此 m 个数 $a_0, a_1, \ldots, a_{m-1}$ 称为模 m 的一个**完全剩余系**(又称**完系**).

由此定义和定理 2.2.1 显然可得到如下定理.

定理 2.2.2 m 个整数 $a_0, a_1, \ldots, a_{m-1}$ 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 2.2.1 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 2.2.3 对于正整数 m,

(1) $0, 1, \ldots, m-1$ 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) $1, 2, \ldots, m-1, m$ 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) $-(m-1), \ldots, -1, 0$ 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) $-m, -(m-1), \ldots, -1$ 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 2.2.3 设 k 是满足$(k, m) = 1$ 的整数, b 是任意整数, 若 $a_0, a_1, \ldots, a_{m-1}$ 是模 m 的一个完全剩余系, 则 $ka_0 + b, ka_1 + b, \ldots, ka_{m-1} + b$ 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 2.2.2, 我们只需要证明当 $a_0, a_1, \ldots, a_{m-1}$ 是模 m 的一个完全剩余系时, m 个整数

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

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

□

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 2.2.4 若 $x_i\ (i=0, 1, \ldots, m_1-1)$是模 m_1 的完全剩余系, $y_j\ (j=0, 1, \ldots, m_2-1)$是模 m_2 的完全剩余系, 其中$(m_1, m_2) = 1$, 则 $m_2 x_i + m_1 y_j\ (i=0, 1, \ldots, m_1-1, j=0, 1, \ldots, m_2-1)$是模 m_1m_2 的完全剩余系.

证明 同样由定理 2.2.2, 我们只需要证明 $m_2x_i + m_1y_j\ (i=0, 1, \ldots, m_1-1, j=0, 1, \ldots, m_2-1)$ 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) $(0 \leqslant a, b \leqslant m_1-1, 0 \leqslant c, d \leqslant m_2-1)$, 且$(x_a, y_c) \neq (x_b, y_d)$, 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 2.2.2 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 2.2

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. 能否写出模 10 的一个完全剩余系, 它的每个数都是奇数（或偶数）?

4. 用模 5 和模 6 的完全剩余系, 表示模 30 的完全剩余系.

5. 求模 11 的一个完全剩余系$\{r_1, r_2, \ldots, r_{11}\}$, 使得 $r_i \equiv 1 \pmod 3$, $1 \leqslant i \leqslant 11$.

6. (1) 把剩余类 1(mod 5)写成模 15 的剩余类之和;

(2) 把剩余类 6(mod 10)写成模 80 的剩余类之和.

B 组

7. 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.

8. 设有 m 个整数, 它们都不属于模 m 的 0 剩余类, 证明其中必有两个数属于同一剩余类.

2.3 欧拉定理和费马小定理

欧拉定理和费马小定理是数论中非常重要的两个定理. 在介绍这两个定理之前，我们先介绍一下相关的概念.

定义 2.3.1 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 2.3.2 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$\{0, 1, \ldots, m-1\}$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 2.3.3 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

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

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, $\{1, 2, \ldots, p-1\}$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 2.3.1 若 $a_1, a_2, \ldots, a_{\varphi(m)}$是$\varphi(m)$个与 m 互素的整数, 则 $a_1, a_2, \ldots, a_{\varphi(m)}$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 2.3.2 若 a 是满足$(a, m)=1$ 的整数, $a_1, a_2, \ldots, a_{\varphi(m)}$是模 m 的一个缩系, 则 $aa_1, aa_2, \ldots, aa_{\varphi(m)}$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, …, $\varphi(m)$), 故$(aa_i, m) = 1$ (i=1, 2, …, $\varphi(m)$). 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, $aa_1, aa_2, \ldots, aa_{\varphi(m)}$, 两两模 m 不同余, 且它们是 $\varphi(m)$ 个不同的整数. 于是, $aa_1, aa_2, \ldots, aa_{\varphi(m)}$ 是模 m 的一个缩系. □

例 2.3.1 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 2.3.3 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 $r_1, r_2, \ldots, r_{\varphi(m)}$ 是模 m 的一个缩系, 则由定理 2.3.2 可知 $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ 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

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

即

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

由于

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

故

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

于是, 根据定理 2.1.6 可得

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

定理得证.

□

定理 2.3.3 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 2.3.4.

定理 2.3.4 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.

□

关于欧拉定理和费马小定理的应用, 我们举两个例子.

例 2.3.2 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 2.3.3 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 2.3.5 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 2.2.4 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 $p|x_1, p|m_1$, 又因为

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

于是 $p|a$, 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 2.2.4 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 2.3.5, 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 2.3.6 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 2.3.5, $m_2x_1 + m_1x_2$ 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 2.3.6, 我们有

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

定理 2.3.7 设 m 有标准分解式

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

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

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

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

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

定理得证.

□

定理 2.3.7 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 2.3.4 求 $\varphi(240)$.

解 $240=2^4\times3\times5$, 所以, $\varphi(240)=240\times(1-\frac{1}{2})(1-\frac{1}{3})(1-\frac{1}{5})=64$.

□

例 2.3.5 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 2.3.6 设$\{x_1,\ x_2,\ \cdots,\ x_{\varphi(m)}\}$是模 m 的缩系, 求证

$$(x_1x_2\cdot\cdots\cdot x_{\varphi(m)})^2\equiv1\ (\mathrm{mod}\ m).$$

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

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

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

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

再由欧拉定理, 推出 $P^2\equiv P^{\varphi(m)}\equiv1\ (\mathrm{mod}\ m)$.

□

例 2.3.7 设 n 是正整数, 记 $F_n=2^{2^n}+1$, 求证 $2^{F_n}\equiv2\ (\mathrm{mod}\ F_n)$.

证明 容易验证, 当 $n\leq4$ 时 F_n 是素数, 所以, 由费马小定理可知结论显然成立.

当 $n\geq5$ 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 $2^{F_n}\equiv2\ (\mathrm{mod}\ F_n)$.

我们已经知道, F_5 是合数, 因此, 例 2.3.7 说明, 费马小定理的逆定理不成立. 即若有整数 a, 且$(a,m)=1$, 使得

$$a^{m-1}\equiv1\ (\mathrm{mod}\ m),$$

并不能保证 m 是素数.

□

我们通常将形如“$a^m \pmod n$”的运算过程称为模幂运算，其在公钥密码学（例如 RSA 公钥加密体制）中有着重要应用. 从前文的讨论中可以看出，欧拉定理可用来简化模幂运算的过程：若$m = k\varphi(n) + r, 0 \le r < \varphi(n)$，则有$a^m \equiv a^{k\varphi(n)+r} \equiv \left(a^{\varphi(n)}\right)^k a^r \equiv a^r \pmod n$，于是我们可以将一个高次模幂运算转化为一个低次模幂运算，从而简化了计算过程.

上述过程中需要对n的欧拉函数$\varphi(n)$进行运算，由定理 2.3.7 可知当已知一个大整数的所有素因子，才能很容易地求出它的欧拉函数值. 然而，在实际应用（特别是密码学）中，n往往是一个很大的整数，我们很难分解出n的素因子（分解出n的素因子的问题称作**大整数分解问题**，详见本书第 9.2 节），因此我们可能无法通过直接应用欧拉定理的方法来简化高次模幂运算. 在这里我们介绍一种密码学中常用的快速求解高次模幂运算的算法——**平方-乘算法**（也称作模重复平方算法）. 算法思路如下：要计算$a^m \pmod n$，设m的二进制表示为

$$\begin{aligned} m &= m_{k-1}2^{k-1} + m_{k-2}2^{k-2} + \cdots + m_1 2^1 + m_0 \\ &= 2(2(\cdots(2(2m_{k-1} + m_{k-2}) + m_{k-3})\cdots) + m_1) + m_0, \end{aligned}$$

于是有

$$\begin{aligned} a^m &\equiv a^{m_{k-1}2^{k-1}+m_{k-2}2^{k-2}+\cdots+m_1 2^1+m_0} \pmod n \\ &\equiv ((\cdots((a^{m_{k-1}})^2 a^{m_{k-2}})^2 \cdots a^{m_2})^2 a^{m_1})^2 a^{m_0} \pmod n. \end{aligned}$$

根据这一表达式，可以设计计算模幂的快速算法，算法过程如下.

算法 2.3.1　平方-乘算法

输入： a，幂次m，模n;

输出： $a^m \pmod n$的结果c;

1. $c \leftarrow 1$;
2. **FOR** $i = k-1$ **TO** 0
3. 　　$c \leftarrow c^2 \pmod n$;
4. 　　**IF** $m_i = 1$ **THEN**
5. 　　　　$c \leftarrow c \cdot a \pmod n$
6. 　　**END IF**
7. **RETURN** c;

例 2.3.8　利用平方-乘算法计算$9726^{3533} \pmod{11413}$.

解　$3533 = (110111001101)_2$，$a = 9726$，下表给出了计算过程.

i	m_i	c
11	1	$1^2 \times 9726 \equiv 9726 \pmod{11413}$
10	1	$9726^2 \times 9726 \equiv 2659 \pmod{11413}$
9	0	$2659^2 \equiv 5634 \pmod{11413}$
8	1	$5634^2 \times 9726 \equiv 9167 \pmod{11413}$
7	1	$9167^2 \times 9726 \equiv 4958 \pmod{11413}$
6	1	$4958^2 \times 9726 \equiv 7783 \pmod{11413}$
5	0	$7783^2 \equiv 6298 \pmod{11413}$
4	0	$6298^2 \equiv 4629 \pmod{11413}$
3	1	$4629^2 \times 9726 \equiv 10185 \pmod{11413}$
2	1	$10185^2 \times 9726 \equiv 105 \pmod{11413}$
1	0	$105^2 \equiv 11025 \pmod{11413}$
0	1	$11025^2 \times 9726 \equiv 5761 \pmod{11413}$

所以，$9726^{3533} \pmod{11413} = 5761$.

□

习题 2.3

A 组

1. 写出以下整数的最小正缩系：

   (1) 6;　　(2) 12;　　(3) 16;　　(4) 17.

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. 利用费马小定理求解以下题目

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

   (2) 解方程 $x^{86} \equiv 6 \pmod{29}$.

   (3) 解方程 $x^{39} \equiv 3 \pmod{13}$.

5. 证明如果$(a, 35) = 1$, 则 $35 \mid (a^{12}-1)$.

6. 证明如果 p 是奇素数, 则$1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}$.

B 组

7. 证明 $2, 2^2, 2^3, \ldots, 2^{18}$ 是模 27 的一个缩系.

8. 证明如果$c_1, c_2, \ldots, c_{\varphi(m)}$是一个模 m 的缩系，其中 m 是一个正整数, 且$m \neq 2$, 则$c_1 + c_2 + \cdots + c_{\varphi(m)} \equiv 0 \pmod{m}$.

9. 证明如果 p 是奇素数, 那么

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

10. 证明如果 a 是整数, 且$(a, 3) = 1$, 那么 $a^7 \equiv a \pmod{63}$.

11. 证明如果 $m>3$, 则 $\varphi(m)$ 总是偶数.

12. 若 p 为素数, n 为整数, 证明 $p \nmid n$ 当且仅当$\varphi(pn) = (p-1)\varphi(n)$.

13. 设 $a>2$ 是奇数, 证明：

    (1) 一定存在正整数 $d \leqslant a-1$, 使得 $a \mid 2^d-1$;

    (2) 若 d_0 是满足(1)的最小正整数, 则 $a \mid 2^h-1$ 的充要条件是 $d_0 \mid h$.

14. $\varphi(m)$“经常”能被 4 整除, 列出所有 $\varphi(m)$ 不能被 4 整除的 m.

15. 证明对于所有的整数 n, 都有 $42 \mid (n^7-n)$成立.

16. 证明如果 a 是非负整数, 那么 $5 \mid 1^n+2^n+3^n+4^n$ 当且仅当 $4 \nmid n$.

17. 编写程序计算给定正整数 n 的欧拉函数.

18. 编写程序构造给定正整数 n 的一个模 n 缩系.

2.4　扩展欧几里德算法和威尔逊定理

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

$$1\times 1 \equiv 1 \pmod{10},$$

$$3\times 7 \equiv 1 \pmod{10},$$

$$9\times 9 \equiv 1 \pmod{10},$$

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 2.4.1 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 2.3.2, 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

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

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

□

由定理 2.4.1 可以很容易地推出：

定义 2.4.1 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 $a^{-1}(\mathrm{mod}\ m)$. 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 1.2 节中介绍的欧几里德算法的基础上发展而来的.

定理 2.4.2 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

$$s_0 = 1, t_0 = 0;$$

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

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

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 $i = 2, 3, \ldots, k-1$ 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 2.4.2 中, $s_n \equiv r_0^{-1} \pmod{r_1}$且 $t_n \equiv r_1^{-1} \pmod{r_0}$. 定理得证.

□

定理 2.4.2 中给出的求乘法逆元的算法称为**扩展欧几里德算法.**

例 2.4.1 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 2.4.2 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$(1\ 769, 550) = 1$, $550^{-1} \equiv 550 \pmod{1\ 769}$, $1\ 769^{-1} \equiv -171 \pmod{550} \equiv 379 \pmod{550}$.

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 2.4.3 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

$$x^2 - 1 \equiv 0 \pmod{p},$$

即

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

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 $x \equiv 1 \pmod{p}$, 由 $p|(x + 1)$可得 $x \equiv -1 \pmod{p}$, 所以方程 $x^2 \equiv 1 \pmod{p}$的解只有 $x \equiv 1 \pmod{p}$和 $x \equiv -1 \pmod{p}$. 定理得证.

□

定理 2.4.3 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 2.4.4 设 p 是一个素数, 则$(p-1)! \equiv -1 \pmod{p}$.

证明 若 $p = 2$, 结论显然成立.

设 $p > 2$, 由定理 2.4.1, 对于每个整数 a, $1 \leqslant a < p$, 存在唯一的整数 a', $1 \leqslant a' < p$, 使得

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

而 $a = a'$充要条件是 a 满足

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

根据定理 2.4.3, 这时有 $a \equiv 1 \pmod{p}$或 $a \equiv p - 1 \pmod{p}$.

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

$$1 \times 2 \times \cdots \times (p-2)(p-1) \equiv 1 \times \prod_{a} aa' \cdot (p-1) \pmod{p}$$

$$\equiv 1 \times (p-1) \pmod{p}$$

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

即$(p-1)!\equiv -1(\mathrm{mod}\ p)$, 定理得证.

□

这个定理又称为**威尔逊定理**. 威尔逊定理给出了判定一个自然数是否为素数的充分必要条件. 感兴趣的读者可以编程验证一下：对于素数 n，$(n\text{-}1)!+1$ 必是素数, 而对于合数 n, $(n\text{-}1)!+1$ 是合数.

习题 2.4

A 组

1. 计算 $8\times9\times10\times11\times12\times13 \pmod 7$.
2. 求 $229^{-1}(\mathrm{mod}\ 281)$.
3. 求 $3\ 169^{-1}(\mathrm{mod}\ 3571)$.
4. 解方程 $105x + 121y = 1$.
5. 证明如果 p 是一个奇素数, 则 $2\times(p-3)\equiv -1\ (\mathrm{mod}\ p)$.

B 组

6. 证明如果 p 为素数, 且 $0<k<p$, 则$(p-k)!\cdot(k-1)!\equiv(-1)^k(\mathrm{mod}\ p)$.
7. 证明如果 p 为素数, 则 $p\mid(a^p+(p-1)!a)$.
8. 证明如果 p 是一个奇素数，则 $2\times(p-3)\equiv -1\ (\mathrm{mod}\ p)$.
9. 设p为素数, 且$a_1,a_2,\ldots,a_p$和$b_1,b_2,\ldots,b_p$为模p的完全剩余系, 证明$a_1b_1,a_2b_2,\ldots,a_pb_p$不是模 p 的一个完全剩余系.
10. 证明正整数n和$n+2$是一对孪生素数，当且仅当$4((n-1)!+1)+n\equiv 0(\mathrm{mod}\ n(n+2)),n\neq 1$.
11. 编写程序判断两个正整数 m, n 是否互素, 如果互素, 求出 $m^{-1}\ (\mathrm{mod}\ n)$和 $n^{-1}\ (\mathrm{mod}\ m)$.
12. 编写程序求所有小于给定正整数 n 的威尔逊素数.