第 2 章　同余

同余是数学中一个重要概念，看似简单，却蕴含着丰富的数学内涵和广泛的应用价值. 通过引入“模”的概念，将整数按照某种规则进行分组，从而通过给定模数下的等价关系简化整数间的关系. 这种分组不仅减少了需要处理的数量，由此衍生出的相关性质还揭示了整数之间更深层次的联系和规律.

剩余类是在同余基础上的进一步延申，是指在模某个正整数下所有同余的整数所组成的集合. 而在该集合中的任意一个整数即为该剩余类的一个代表元，进而可以从所有剩余类中各取一个代表元，组成一个完全剩余系. 此外，还可以去除完全剩余系中的一些“冗余“元素，构成一个简化剩余系. 它们使得在特定模下的运算更加高效，在数论、密码学、信息安全等领域都有着广泛的应用.

在探讨剩余类的过程中，我们将介绍与简化剩余系密切相关的欧拉函数，它不仅在数论中有着重要的地位，还在密码学等领域的许多算法中发挥着关键作用. 我们将介绍几个重要的定理：欧拉定理、费马小定理和 Wilson 定理. 这些定理揭示了同余理论中的深刻联系和规律，为我们利用同余理论解决问题提供了强有力的支持.

最后，我们还特别介绍模重复平方计算法，也称为模幂运算的快速算法，广泛应用于密码学中的加密和解密过程。

总之，本章通过深入探讨同余的概念、基本性质、剩余类及相关定理和算法，为读者构建一个理解模运算及其应用的完整框架，并为后续学习打下坚实的基础。

本章的知识要点：

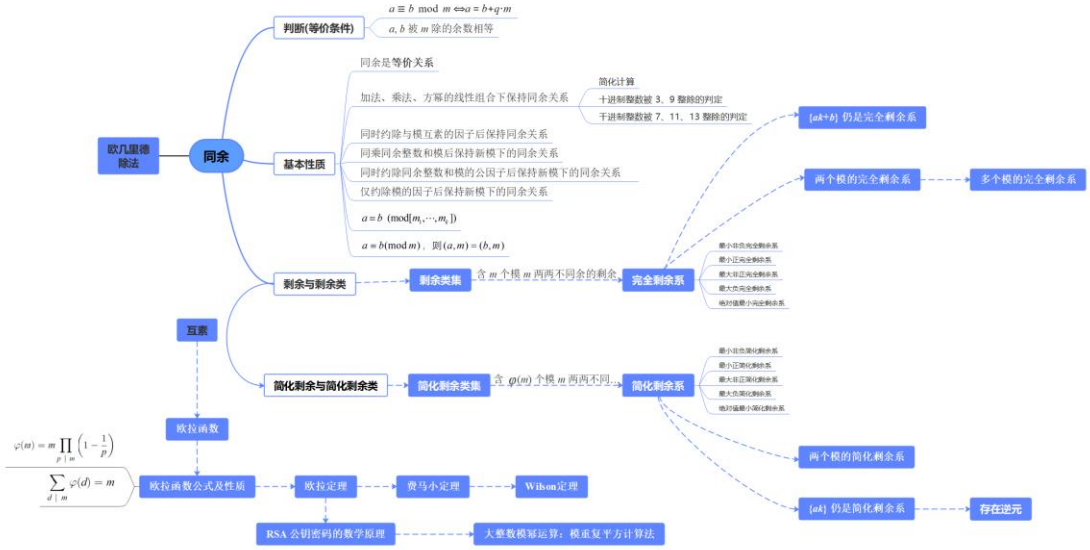

图 2-1 同余知识点图谱

2.1 同余的概念及基本性质

上一章我们讨论了整数间的除法运算，现在我们讨论整数的同余关系，并由此对整数进行恰当的分类.

2.1.1 同余的概念

同余的概念常常出现于日常生活中**.** 例如，每星期是模 7（天），每天是模 24（小时），每小时是模 60（分钟），每分钟也是模 60（秒）.

定义 2.1.1 给定一个正整数 m，两个整数 a, b 叫做**模 *m* 同余**，如果 $a-b$ 被 m 整除，或 $m|a-b$，记作 $a \equiv b \pmod m$;

否则，叫做**模 *m* 不同余.** 记作 $a \not\equiv b \pmod m$**.**

注 模 m 是一个正整数，在同余性质的讨论中为一个固定整数.

例 2.1.1 例如: (1) $100 \equiv 2 \pmod 7$， 因为 $7|100-2$**.**

(2) $1000 \equiv -1 \pmod 7$ 和 $10000 \equiv 4 \pmod 7$**.**

如何判断两个整数 *a*，*b* 模 *m* 同余呢?

可以直接运用同余的定义，即计算 $a-b$ 被模 m 除的余数，此时需要使用欧几里德除法。此外，我们再引进一些等价的判别法，用来判断两个整数 a，b 模 m 是否同余.

定理 2.1.1 设 m 是一个正整数，a，b 是两个整数，则 $a \equiv b \pmod m$ 的充要条件是存在一个整数 k 使得 $a=b+km$.

证 如果 $a \equiv b \pmod m$，则根据同余的定义，我们有 $m|a-b$.

根据整除的定义，存在一个整数 k 使得 $a-b=km$. 故 $a=b+km$.

反过来，如果存在一个整数 k 使得 $a=b+km$，则有 $a-b=km$.

根据整除定义，我们有 $m|a-b$.

再根据同余的定义 2.1.1，我们得到 $a \equiv b \pmod m$.

例 2.1.2 我们有 $2024 \equiv 1 \pmod 7$，因为 $2024=289 \cdot 7+1$.

定理 2.1.2 整数 a，b 模 m 同余的充分必要条件是 a，b 被 m 除的余数相同.

证 根据欧几里德除法，分别存在整数 q，r 和 q'，r'使得

$$a = qm+r, \qquad 0\le r < m.$$

$$b = q'm+ r', \qquad 0\le r' < m.$$

两式相减，得到 $a-b=(q-q')m+(r-r')$.

或者 $(r-r')=a-b-(q-q')m$.

因此，$m|a-b$ 的充分必要条件是 $m|r-r'$.

但因为 $0\le|r-r'|<m$，且 $m|r-r'$的充分必要条件是 $r-r'=0$,

所以 $m|a-b$ 的充分必要条件是 $r-r'=0$.

例 2.1.3 有 $2024\equiv 1485\ (mod\ 7)$，因为 $2024\equiv 289\cdot 7+1$，$1485=212\cdot 7+1$.

例 2.1.4 单表密码.

首先建立英文字母和模数 26 的剩余之间的对应关系，如表 2-1 所示.

表 2-1 英文字母和模数 26 的剩余之间的对应关系

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

1) 移位密码：将每个字母对应的数字后移若干位作为密文字母对应的数字. 如凯撒（Caesar）密码，将每个字母后移 3 位，

如：thiscryptosystemisnotsecure 加密后为 wklvfubswrvbvwhplvqrwvhfxuh,

这相当于把每个字母对应的数字加 3 后取模数 26，再将所有的余数对应回字母，即把 thiscryptosystemisnotsecure 对应的数字 19，7，8，18，2，17，24，15，19，14，18，24，18，19，4，12，8，18，13，14，19，18，4，2，20，17，4 分别加 3 后取模数 26，所得的余数 22，10，11，21，5，20，1，18，22，17，21，1，21，22，7，15，11，21，16，17，22，，21，7，5，23，20，7，在对应回字母 wklvfubswrvbvwhplvqrwvhfxuh.

用公式表达为 $E\equiv P+3\pmod{26}$，其中 P 为明文字母对应的数字，E 为密文字母对应的数字. 显然解密时使用公式 $P=E-3\,(\mathrm{mod}\,26)$，即每个密文字母前移 3 位.

这种密码极易破译. 仅统计标出最高频度字母，再与明文字母表字母对应决定出移位量，就可以得到正确解.

2) 仿射密码：将每个字母对应的数字乘以 k 后再加 b 作为密文字母对应的数字.

当 k=7，b=6 时，如 thiscryptosystemisnotsecure，加密后为 jdkcuvshjacscjimkctajciuqvi,

这相当于把字母把每个字母对应的数字乘以 7 后加 6 并取模数 26，再将所得的余数对应回字母，即把 thiscryptosystemisnotsecure 对应的数字 19，7，8，18，2，17，24，15，19，14，18，24，18，19，4，12，8，18，13，14，19，18，4，2，20，17，4 分别乘以 7 后加

6 并取模数 26，所得的余数 9，3，10，2，20，21，18，7，9，0，2，18，2，9，8，12，10，2，19，0，92，8，20，16，21，8，再对应回字母 jdkcuvshjacscjimkctajciuqvi. 用公式表达为 $E \equiv 7P + 6(\mathrm{mod}\ 26)$，其中 P 为明文字母对应的数字，E 为密文字母对应的数字. 显然，由于 $7\times 15 \equiv 1(\mathrm{mod}\ 26)$，解密时使用公式 $P = 15E + 14\ (\mathrm{mod}\, 26)$.

这种密码虽然要复杂些, 但多虑几个密文字母统计表与明文字母表的匹配关系也不难解出.

2.1.2 同余的基本性质

模同余具有等价关系的性质.

性质 2.1.1 模 m 同余是等价关系，即

（i）（自反性）对任一整数 a，　则 $a \equiv a$ （$mod\ m$）;

（ii）（对称性）若 $a \equiv b$ （$mod\ m$），则 $b \equiv a$ （$mod\ m$）;

（iii）（传递性）若 $a \equiv b$ （$mod\ m$），$b \equiv c$ （$mod\ m$），则 $a \equiv c$ （$mod\ m$）.

证　运用定理 2.1.1.

（i）（自反性）对任一整数 a，我们有 $a=a+0\cdot m$，所以 $a \equiv a$ （$mod\ m$）.

（ii）（对称性）若 $a \equiv b$ （$mod\ m$），则存在整数 k 使得 $a=b+km$，

从而有 $b=a+(-k)m$.

因此，$b \equiv a$（$mod\ m$）.

（iii）（传递性）若 $a \equiv b$ （$mod\ m$），$b \equiv c$ （$mod\ m$），

则分别存在整数 k_1，k_2 使得 $a=b+k_1 m$，　$b=c+k_2 m$.

从而有 $a=c+(k_1+k_2)m$.

因为 k_1+k_2 是整数，所以 $a \equiv c$ （$mod\ m$）.

例 2.1.5 因为 $2024 \equiv 1485$（$mod\ 7$），$1485 \equiv 715$（$mod\ 7$），所以

$2024 \equiv 715$（$mod\ 7$）. 传递性

同时，我们有

$2024 \equiv 2024$（$mod\ 7$），　$1485 \equiv 1485$ ($mod\ 7$)，　$715 \equiv 715$ ($mod\ 7$). 自反性

以及

$1485 \equiv 2024$（$mod\ 7$），　$715 \equiv 1485$ ($mod\ 7$). 对称性

因为模同余是等价关系，所以我们有整数 a，b 模 m 的加法运算和乘法运算的性质.

性质 2.1.2 设 m 是一个正整数，a_1，a_2，b_1，b_2，是四个整数. 如果

$$a_1 \equiv b_1 \ (mod\ m), \qquad a_2 \equiv b_2 \ (mod\ m)$$

则（i）$a_1+a_2 \equiv b_1+b_2 \ (mod\ m)$；

（ii）$a_1\ a_2 \equiv b_1\ b_2 \ (mod\ m)$.

证 依题设，根据定理 2.1.1，分别存在整数 k_1，k_2 使得

$$a_1=b_1+k_1\ m, \qquad a_2=b_2+k_2\ m.$$

从而

$$a_1+a_2=b_1+b_2+(k_1+k_2)m.$$

$$a_1\ a_2=b_1\ b_2+\ (k_1\ b_2+k_2\ b_1+k_1\ k_2\ m)\ m.$$

因为 k_1+k_2，$k_1\ b_2+k_2\ b_1+k_1\ k_2\ m$ 都是整数，

所以根据定理 2.1.1，我们有

$$a_1+a_2 \equiv b_1+b_2 \ (mod\ m)$$

$$a_1\ a_2 \equiv b_1\ b_2 (mod\ m)$$

即定理成立.

例 2.1.6 已知 $2024 \equiv 1\ (mod\ 7)$，$1000 \equiv -1\ (mod\ 7)$，所以

$3024=2024+1000 \equiv 1+(-1) \equiv 0\ (mod\ 7)$，　　$1024=2024-1000 \equiv 1-(-1) \equiv 2\ (mod\ 7)$,

$2024000=2024 \cdot 1000 \equiv 1 \cdot (-1) \equiv -1\ (mod\ 7)$，　　$4096576=2024^2 \equiv 1^2 \equiv 1\ (mod\ 7)$,

$1000000=1000^2 \equiv (-1)^2 \equiv 1\ (mod\ 7)$.

例 2.1.7 2024 年 9 月 1 日是星期日，问第 2^{2024} 天后是星期几?

解 因为

$$2^1 \equiv 2\ (mod\ 7), \ 2^2 \equiv 4\ (mod\ 7), \ 2^3=8 \equiv 1(mod\ 7).$$

又 $2024=674 \cdot 3+2$，所以

$$2^{2024}=(2^3)^{674} \cdot 2^2 \equiv 1 \cdot 4 \equiv 4\ (mod\ 7).$$

故第 22024 天后是星期四.

推论 2.1.1 若 $x \equiv y\ (mod\ m)$，$a_i \equiv b_i (mod\ m)$，$0 \le i \le k$，则

$$a_0+a_1x+...+a_kx^k \equiv b_0+b_1y+...+b_ky^k \ (mod\ m).$$

证 设 $x \equiv y\ (mod\ m)$，由性质 2.1.2，我们有 $x^i \equiv y^i \ (mod\ m)$，$0 \le i \le k$.

又 $a_i \equiv b_i \ (mod\ m)$，（$0 \le i \le k$）．将它们对应相乘，我们有

$$a_i x^i \equiv b_i y^i \ (mod\ m),\ 0 \le i \le k.$$

最后，将这些式子左右对应相加，得到

$$a_0 + a_1 x + ... + a_k x^k \equiv b_0 + b_1 y + ... + b_k y^k \ (mod\ m).$$

推论 2.1.1 可以帮助我们很快地判断一些数是否被 3 或 9 整除.

推论 2.1.2 设整数 n 有十进制表示式:

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

则 $3|n$ 的充分必要条件是 $3|a_k + ... + a_0$;

而 $9|n$ 的充分必要条件是 $9|a_k + ... + a_0$.

证 因为 $10 \equiv 1 \ (mod\ 3)$，又 $1^i = 1$，$0 \le i \le k$. 所以，根据推论 2.1.1，我们有

$$a_k 10^k + a_{k-1} 10^{k-1} + ... + a_1 10 + a_0 \equiv a_k + ... + a_0 \ (mod\ 3).$$

因此，$a_k 10^k + a_{k-1} 10^{k-1} + ... + a_1 10 + a_0 \equiv 0 \ (mod\ 3)$.

的充分必要条件是 $a_k + ... + a_0 \equiv 0 \ (mod\ 3)$.

结论对于 m=3 成立.

同理，对于 m=9，结论也成立.

例 2.1.8 设 n=20240901，则 $3|n$，$9|n$.

解 因为 $a_k + ... + a_0$ =2+2+4+9+1=18.

又 3|18，9|18，根据推论 2.1.2，我们有 $3|n$，$9|n$.

例2.1.9 设 n=20240922，则 n 被 3 整除，但不被 9 整除.

解 因为 $a_k + ... + a_0$ =2+2+4+9+2+2=21=3·7,

又 $3|3\cdot 7$，$9 \nmid 3\cdot 7$，根据推论 2.1.2，我们有 $3|n$，$9 \nmid n$.

同时，推论 2.1.1 可以帮助我们很快地判断一些数是否被 7（或 11，或 13）整除.

推论 2.1.3 设整数 n 有 1000 进制表示式: $a_k 1000^k + ... + a_1 1000 + a_0$, $0 \le a_i < 1000$.

则 7(或 11，或 13)|n 的充分必要条件是:

7（或 11，或 13）能整除整数 $(a_0 + a_2 + ...) - (a_1 + a_3 + ...)$.

证 因为 $1000=7\cdot 11\cdot 13-1\equiv -1\ (mod\ 7)$

所以 $1000\equiv 1000^3\equiv 1000^5\equiv \ldots\equiv -1\ (mod\ 7)$，

以及 $1000^2\equiv 1000^4\equiv 1000^6\equiv \ldots\equiv 1\ (mod\ 7)$.

根据推论 2.1.1，得到

$$a_k 1000^k + a_{k-1}1000^{k-1} + \ldots + a_1 1000 + a_0$$

$$\equiv a_k(-1)^k + a_{k-1}(-1)^{k-1} + \ldots + a_1(-1) + a_0$$

$$\equiv (a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots) \qquad (mod\ 7).$$

因此，$7|n$ 的充分必要条件是 $7|(a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots)$，

即结论对于 $m=7$ 成立.

同理，结论对于 $m=11$ 或 13 也成立.

例 2.1.10 设 $n=20240920$，则 n 被 7 整除，但不被 11, 13 整除.

解 因为 $n = 20\cdot 1000^2+240\cdot 1000+920$,

又 $(a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots) = 920+20-240 = 700 = 2^2\cdot 5^2\cdot 7$,

所以 n 被 7 整除，但不被 11， 13 整除.

例 2.1.11 设 $n=20240922$，则 n 被 13 整除，但不被 7， 11 整除.

解 因为 $n = 20\cdot 1000^2+240\cdot 1000+922$,

又 $(a_0 + a_2 + \ldots) - (a_1 + a_3 + \ldots) = 922+20-240 = 702 = 2\cdot 3^3\cdot 13$,

所以 n 被 13 整除，但不被 7， 11 整除.

性质 2.1.3 设 m 是一个正整数， $ad \equiv bd(\mathrm{mod}\, m)$. 如果（$d$，$m$）=1，则 $a \equiv b(\mathrm{mod}\, m)$.

证 若 $ad \equiv bd(\mathrm{mod}\, m)$，则 $m \mid ad - bd$，即 $m \mid d(a-b)$.

因为（d，m）=1，根据定理 1.2.8,

我们有 $m|a-b$，结论成立.

例 2.1.12 因为 $1485\equiv 715\ (mod\ 7)$, $(5, 7) = 1$, $95 \equiv 25(\mathrm{mod}\, 7), (5,7) = 1,$ 所以 $297\equiv 143\ (mod\ 7)$.

性质 2.1.4 设 m 是一个正整数，如果 $a \equiv b(\mathrm{mod}\, m)$, $k>0$, 则

$$ak \equiv bk(\bmod mk).$$

证 如果$a \equiv b(\bmod m)$，则存在整数 q，使得

$$a=b+qm.$$

进而 $ak=bk+qmk$，　　因此 $ak=bk+q(mk)$,

根据定理 2.1.1 有：　$ak \equiv bk(\bmod mk)$．结论成立.

例 2.1.13 因为 31≡3 (*mod* 7), k = 5>0, 所以 155≡15 (*mod* 35).

性质 2.1.5　设 m 是一个正整数，$a \equiv b(\bmod m)$．如果整数 $d|(a, b, m)$，则

$$\frac{a}{d} \equiv \frac{b}{d}(\bmod \frac{m}{d}).$$

证　因为 $d|(a, b, m)$，所以存在整数a', b', m',使得

$$a = da', \quad b = db', \quad m = dm'.$$

现在$a \equiv b(\bmod m)$，所以存在整数 k 使得 $a=b+mk$,

即 $da' = db' + dm'k$.

因此 $a' = b' + m'k$.

这就是 $a' \equiv b'(\bmod m')$,

或者 $\frac{a}{d} \equiv \frac{b}{d}(\bmod \frac{m}{d})$.

例 2.1.14 因为 155≡15 (*mod* 35)，所以取 d=5，得到 31≡3 (*mod* 7).

性质 2.1.6　设 m 是一个正整数，$a \equiv b(\bmod m)$．如果 $d|m$，则 $a \equiv b(\bmod d)$.

证　因为 $d|m$，所以存在整数m'使得$m = dm'$．又因为$a \equiv b(\bmod m)$，

所以存在整数 k 使得 $a=b+mk$.

该式又可以写成 $a = b + d(m'k)$.

故 $a \equiv b(\bmod d)$.

例 2.1.15 因为 169≡29 (*mod* 35)，所以取 d=7，得到 169≡29 (*mod* 7).

性质 2.1.7 设 m 是一个正整数，$a \equiv b \ (\bmod m_i), \ i = 1, \cdots, k,$ 则

$$a \equiv b \ (\bmod[m_1, \cdots, m_k]).$$

证 设 $a \equiv b(\mathrm{mod}\, m_i),\ i=1,\cdots,k,$ 则 $m_i \mid a-b,\ i=1,\cdots,k,$

根据定理 1.2.14，我们有 $[m_1,\cdots,m_k] \mid a-b$.

即 $a \equiv b(\mathrm{mod}[m_1,\cdots,m_k])$.

例 2.1.16 因为 155≡15 (*mod* 5), 155≡15 (*mod* 7), (5, 7) =1, [5, 7]=35, 所以 155≡15 (*mod* 35).

性质 2.1.8 设 *m* 是一个正整数，$a \equiv b(\mathrm{mod}\, m)$，则 $(a,m)=(b,m)$.

证 设 $a \equiv b(\mathrm{mod}\, m)$，则存在整数 *k* 使得 *a=b+mk.*

根据定理 1.2.2，我们有 $(a,m)=(b,m)$.

2.2 剩余类

同余是一种等价关系，因此可以借助同余对全体整数进行分类，并将每类作为一个"数"来看待，进而得到一些新性质.

2.2.1 剩余及剩余类

设 *m* 是一个正整数，对任意整数 *a*，令

$$C_a = \{c \mid c \in Z,\quad a \equiv c(\mathrm{mod}\, m)\} \tag{2.2.1}$$

C_a 是非空集合，因为 $a \in C_a$.

定义 2.2.1 C_a 叫做模 *m* 的 *a* 的**剩余类**. 一个剩余类中的任一数叫做该类的**剩余 (**或**代表元)**.

定理 2.2.1 设 *m* 是一个正整数，则

(*i*) 任一整数必包含在一个 C_r 中，$0 \le r \le m-1$;

(*ii*) $C_a = C_b$ 的充分必要条件是 $a \equiv b(\mathrm{mod}\, m)$;

(*iii*) C_a 与 C_b 的交集为空集的充分必要条件是 $a \not\equiv b(\mathrm{mod}\, m)$.

证 (*i*) 设 *a* 为任一整数，根据欧几里德除法，

存在惟一的整数 *q*，*r* 使得 $a = mq + r,\quad 0 \le r < m$.

因此，我们有 $r \equiv a(\mathrm{mod}\, m)$，*a* 包含在 C_r 中.

(*ii*) 因为 $b \in C_b = C_a$，所以必要性成立.

充分性：设整数 *a*，*b* 满足关系式 (2.2.1)，即 $a \equiv b(\mathrm{mod}\, m)$.

要证明：$C_a = C_b$，对任意的整数$c \in C_a$，我们有 $a \equiv c(\mathrm{mod}\, m)$.

由（i）式及性质 2.1.1（ii）（对称性），我们有 $b \equiv a(\mathrm{mod}\, m)$.

再由性质 2.1.1（iii）（传递性），我们得到$b \equiv c(\mathrm{mod}\, m)$.

这说明，$c \in C_b$ 以及$C_a \sqsubset C_b$.

同样，对任意的整数$c \in C_b$，我们有$b \equiv c(\mathrm{mod}\, m)$.

由式（2.2.1）及性质 2.1.1（iii）（传递性），我们得到$a \equiv c(\mathrm{mod}\, m)$.

这说明，$c \in C_b$ 以及$C_b \sqsubset C_a$.

故$C_a = C_b$.

（iii）由（ii）立即得到必要性.

充分性：反证法.

假设C_a与C_b的交集非空，即存在整数 c 满足$c \in C_a$及$c \in C_b$，

则我们有 $a \equiv c(\mathrm{mod}\, m)$及$b \equiv c(\mathrm{mod}\, m)$.

对于$b \equiv c(\mathrm{mod}\, m)$，应用性质 2.1.1（$ii$）（对称性），我们有 $c \equiv b(\mathrm{mod}\, m)$.

再由性质 2.1.1（iii）（传递性），我们得到 $a \equiv b(\mathrm{mod}\, m)$.

这与假设矛盾，故C_a与C_b的交集为空集.

2.2.2 完全剩余系

定义 2.2.2 若$r_0, r_1, \cdots, r_{m-1}$是 m 个整数，并且其中任何两个数都不在同一剩余类里，则$r_0, r_1, \cdots, r_{m-1}$叫做模 m 的一个**完全剩余系**.

根据定义，模 m 的剩余类有 m 个：$C_0, C_1, \cdots, C_{m-1}$.

例 2.2.1 设正整数 m=12. 对任意整数 a，集合

$$C_a = \{a+12k | k \in \boldsymbol{Z}\}$$

是模 m=12 的剩余类.

则完全剩余系为：

0，1，2，3，4，5，6，7，8，9, 10, 11 为模 12 的一个完全剩余系.

1，2，3，4，5，6，7，8，9，10, 11, 12 为模 12 的一个完全剩余系.

0，-1，-2，-3，-4，-5，-6，-7，-8，-9, -10, -11 为模 12 的一个完全剩余系.

0，5，10，15，20，25，30，35，40，45, 50, 55 为模 12 的一个完全剩余系.

12，13，26，39，52，65，78，91，104，117, 130, 143 为模 12 的一个完全剩余系.

定理 2.2.2 设 m 是一个正整数，则 m 个整数 $r_0, r_1, \cdots, r_{m-1}$ 为模 m 的一个完全剩余系的充分必要条件是它们模 m 两两不同余.

证 设 $r_0, r_1, \cdots, r_{m-1}$ 是模 m 的一个完全剩余系，

根据定理 2.2.1（*ii*），它们模 m 两两不同余.

反过来，设 $r_0, r_1, \cdots, r_{m-1}$ 模 m 两两不同余.

根据定理 2.2.1（*iii*），这 m 个整数中的任何两个整数都不在同一个剩余类里.

因此，它们成为模 m 的一个完全剩余系.

定义 2.2.3 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，

$$-m/2, -(m-2)/2, \cdots, -1, 0, 1, \cdots, (m-2)/2$$

或

$$-(m-2)/2, \cdots, -1, 0, 1, \cdots, (m-2)/2, m/2$$

是模 m 的一个完全剩余系；

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

定理 2.2.3 设 m 是正整数，a 是满足（a，m）=1 的整数，b 是任意整数. 若 x 是遍历模 m 的一个完全剩余系，则 $ax+b$ 也遍历模 m 的一个完全剩余系.

证 根据定理 2.2.2，我们只需证明：当 $a_0, a_1, \cdots, a_{m-1}$ 是模 m 的一个完全剩余系时，

m 个整数 $aa_0+b, \quad aa_1+b, \quad \cdots, \quad aa_{m-1}+b$ 模 m 两两不同余.

如果，存在 a_i 和 $b_j (i \neq j)$ 使得 $aa_i + b \equiv aa_j + b \pmod{m}$.

则 $m \mid a(a_i - a_j)$. 因为（a，m）=1，我们有 $m \mid a_i - a_j$，

这说明 a_i 与 a_j 模 m 同余，与假设矛盾.

因此，$ax+b$ 也遍历模 m 的一个完全剩余系.

例 2.2.2 设 m=12，a=5，b=3，则形为 $ax+b$ 的 12 个数:

3，8，13，18，23，28，33，38，43，48, 53, 58 构成模 12 的一个完全剩余系.

定理 2.2.4 设 m_1, m_2 是两个互素的正整数，若 x_1, x_2 分别遍历模 m_1, m_2 的完全剩余系，则 $m_2x_1 + m_1x_2$ 遍历模 m_1m_2 的完全剩余系.

证 因为 x_1, x_2 分别遍历 m_1, m_2 个数时， $m_2x_1 + m_1x_2$ 遍历 m_1m_2 个整数，

所以只需证明这 m_1m_2 个整数模 m_1m_2 两两不同余.

如果，若整数 x_1, x_2 和 y_1, y_2 满足

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

则根据性质 2.1.6，我们有 $m_2x_1 + m_1x_2 \equiv m_2y_1 + m_1y_2 \pmod{m_1}$

或者 $m_2x_1 \equiv m_2y_1 \pmod{m_1}$.

进而， $m_1 \mid m_2(x_1 - y_1)$.

因为 $(m_1, m_2) = 1$，所以 $m_1 \mid x_1 - y_1$，故 x_1 与 y_1 模 m_1 同余.

同理， x_2 与 y_2 模 m_2 同余. 因此，结论成立.

例 2.2.3 设 p，q 是两个不同的素数，n 是它们的乘积，则对任意的整数 c，存在惟一的一对整数 x，y 满足 $qx + py \equiv c \pmod{n}, \quad 0 \le x < p, 0 \le y < q$.

证 因为 p，q 是两个不同的素数，所以 p，q 是互素的.

根据定理 2.2.4 及其证明知，x，y 分别遍历模 p，q 的完全剩余系时，

$qx + py$ 遍历模 $n = pq$ 的完全剩余系.

因此，存在惟一的一对整数 x，y 满足

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

2.2.3 简化剩余系及欧拉函数

这节，我们讨论剩余 a 与模 m 互素的剩余类的情况.

定义 2.2.4 设 m 是一个正整数，则 m 个整数 0，1，…，m-1 中与 m 互素的整数的个数，记作 $\varphi(m)$，通常叫做欧拉（*Euler*）函数.

例 2.2.4 设 m=12，则 12 个整数 0，1，2，3，4，5，6，7，8，9, 10, 11 中与 12 互素的整数为 1，5，7，11. 所以$\varphi(12)=4$.

例 2.2.5 当 $m=p$ 为素数时，则 1，2，…，p-1，p 中与 p 互素的整数为 1，2，…，p-1. 所以$\varphi(p)=p-1$.

定理 2.2.5 对于$n=p^{\alpha}$ 素数幂时，$\varphi(p^{\alpha})= p^{\alpha}-p^{\alpha-1}=p^{\alpha-1}(p-1)$.

证 当$n=p^{\alpha}$ 素数幂时，从 1 到 n 的整数为

$$\begin{array}{llll} 0, & 1, & \cdots, & p-1 \\ \cdots\cdots & & & \\ p(p^{\alpha-1}-1) & p(p^{\alpha}-1)+1, & \cdots, & p^{\alpha}-1 \end{array}.$$

共有$n=p^{\alpha}$ 个整数，其中与 n 不互素的整数为

$$p\cdot 0,\quad p\cdot 1,\quad \cdots,\quad p(p^{\alpha-1}-1)$$

共有 $p^{\alpha-1}$ 个整数，因此，$\varphi(p^{\alpha})= p^{\alpha}-p^{\alpha-1}=p^{\alpha-1}(p-1)$.

例 2.2.6 设 $m=7^3$， 则 m 的欧拉函数值为 294.

定义 2.2.5 如果一个模 m 的剩余类中，存在一个与 m 互素的剩余，则该剩余类叫做**简化剩余类**.

注：这个定义与剩余类中剩余的选取无关.

定理 2.2.6 设 r_1, r_2 是同一模 m 剩余类的两个剩余，则 r_1 与 m 互素的**充分必要**条件是 r_2 与 m 互素.

证 依题设，我们有 $r_1=r_2+km$.

根据定理 1.2.2，$(r_1,m)=(r_2,m)$.

因此，$(r_1,m)=1$ 的充分必要条件是 $(r_2,m)=1$.

定义 2.2.6 设 m 是一个正整数，在模 m 的所有不同简化剩余类中，从每个类任取一个数组成的整数的集合，叫做模 m 的一个**简化剩余系**.

由定义可知，模 m 的一个简化剩余系的元素的个数为 $\varphi(m)$.

定义 2.2.7 设 m 是一个正整数，则

（i）m 个整数 $0,1,\cdots,m-1$ 中与 m 互素的整数全体组成模 m 的一个简化剩余系，叫做模 m 的**最小非负简化剩余系**；

（ii）m 个整数 $1,\cdots,m-1,m$ 中与 m 互素的整数全体组成模 m 的一个简化剩余系，叫做模 m 的**最小正简化剩余系**；

（iii）m 个整数 $-(m-1),\cdots,-1,0$ 中与 m 互素的整数全体组成模 m 的一个简化剩余系，叫做模 m 的**最大非正简化剩余系**；

（iv）m 个整数 $-m,-(m-1),\cdots,-1$ 中与 m 互素的整数全体组成模 m 的一个简化剩余系，叫做模 m 的**最大负简化剩余系**；

（v）m 个整数 $1,\cdots,m-1,m$ 中与 m 互素的整数全体组成模 m 的一个简化剩余系，叫做模 m 的**最小正简化剩余系**；

（vi）当 m 分别为偶数时，m 个整数

$$-m/2,-(m-2)/2,\cdots,-1,0,1,\cdots,(m-2)/2$$

或 m 个整数 $-(m-2)/2,\cdots,-1,0,1,\cdots,(m-2)/2,m/2$

中与 m 互素的整数全体组成模 m 的一个简化剩余系.

当 m 分别为奇数时，m 个整数 $-(m-1)/2,\cdots,-1,0,1,\cdots,(m-1)/2$ 中与 m 互素的整数全体组成模 m 的一个简化剩余系.

上述两个简化剩余系统称为模 m 的一个**绝对值最小简化剩余系**.

例 2.2.7 1，7，11，13，17，19，23，29 是模 30 的简化剩余系，$\varphi(30)=8$.

例 2.2.8 1，2，3，4，5，6, 7, 8, 9, 10, 11, 12 是模 13 的简化剩余系，$\varphi(13)=12$.

注：当 $m=p$ 为奇数时 1，2，…，p-1 是模 p 的简化剩余系，所以 $\varphi(p)=p-1$.

定理 2.2.7 设 m 是一个正整数，若 $r_1,\cdots,r_{\varphi(m)}$ 是 $\varphi(m)$ 个与 m 互素的整数，并且两两模 m 不同余，则 $r_1,\cdots,r_{\varphi(m)}$ 是模 m 的一个简化剩余系.

证 根据定理的假设条件及定理 2.2.1 知，$\varphi(m)$ 个整数 $r_1,\cdots,r_{\varphi(m)}$ 是模 m 的所有不同简化剩余类的剩余.

因此，$r_1,\cdots,r_{\varphi(m)}$ 是模 m 的一个简化剩余系.

定理 2.2.8 设 m 是一个正整数，a 是满足（a，m）=1 的整数. 如果 x 遍历模 m 的一个简化剩余系，则 ax 也遍历模 m 的一个简化剩余系.

证 因为（a，m）=1，（x，m）=1，根据推论 1.2.1，我们有（ax，m）=1

这说明 ax 是简化剩余类的剩余.

又 $ax_1 \equiv ax_2 \pmod{m}$ 时，有 $x_1 \equiv x_2 \pmod{m}$.

因此，x 遍历模 m 的一个简化剩余系时，ax 遍历 $\varphi(m)$ 个数，且它们两两模 m 不同余. 根据定理 2.2.7，ax 遍历模 m 的一个简化剩余系.

例 2.2.9 已知 1，7，11，13，17，19，23，29 是模 30 的简化剩余系，（7，30）=1，所以

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

因此，$7\cdot 1$，$7\cdot 7$，$7\cdot 11$，$7\cdot 13$，$7\cdot 17$，$7\cdot 19$，$7\cdot 23$，$7\cdot 29$ 是模 30 的简化剩余系.

例 2.2.10 设 m=7，a 表示第一列数，为与 m 互素的给定数，x 表示第一行数，遍历模 m 的简化剩余系，a 所在行与 x 所在列的交叉位置表示 ax 模 m 最小非负剩余. 则我们得到如下的列表:

a \ x	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

其中 a 所在行的数表示 ax 随 x 遍历模 m 的简化剩余系.

定理 2.2.9 设 m 是一个正整数，a 是满足（a，m）=1 的整数，则存在整数 $a', 1 \le a' < m$ 使得 $aa' \equiv 1 \pmod{m}$.

证一（存在性证明）

因为（a，m）=1，根据定理 2.2.8，x 遍历模 m 的一个最小简化剩余系时，ax 也遍历模 m 的一个简化剩余系.

因此，存在整数 $x = a', 1 \le a' < m$ 使得 aa' 属于 1 的剩余类，即 $aa' \equiv 1 \pmod{m}$.

证二（构造性证明）

因为在实际运用中，我们常常需要具体地求出整数，所以我们运用广义欧几里德除法给出该定理的构造性证明.

因为（a，m）=1，运用广义欧几里德除法，

我们可找到整数 s，t 使得 $sa+tm$=（a，m）=1.

因此，整数 $a' \equiv s \pmod{m}$ 满足 $aa' \equiv 1 \pmod{m}$.

例 2.2.11 设 m=7，a 表示与 m 互素的整数. 根据定理 2.2.9，我们得到：

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

例 2.2.12 设 m=65521，a=32749.

由广义欧几里德除法，可找到整数 s=11391，t=-22790 使得 11391·65521-22790·32749 = 1.

因此，a' = -22790 ≡ 42731 (mod 65521) 使得 42731·32749 ≡1 (mod 65521).

定理 2.2.10 设 m_1, m_2 是互素的两个正整数. 如果 x_1, x_2 分别遍历模 m_1 和模 m_2 的简化剩余系，则 $m_2x_1 + m_1x_2$ 遍历 m_1m_2 的简化剩余系.

证 首先，$(x_1, m_1) = 1, (x_2, m_2) = 1$ 时，$(m_2x_1 + m_1x_2,\ m_1m_2) = 1$

事实上，因为 $(m_1, m_2) = 1$，根据定理 1.2.2 和定理 1.2.8，我们有

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

因此，再根据推论 1.2.1，我们得到 $(m_2x_1 + m_1x_2,\ m_1m_2) = 1$

其次，证明模 m_1m_2 的任一简化剩余可表示为

$$m_2x_1 + m_1x_2 \qquad \text{其中：}\ (x_1, m_1) = 1,\ \ (x_2, m_2) = 1.$$

事实上，根据定理 2.2.4，模 m_1m_2 的任一剩余可以表示为 $m_2x_1 + m_1x_2$.

因此，当 $(m_2x_1 + m_1x_2,\ m_1m_2) = 1$ 时，我们有

$$(x_1, m_1) = (m_2x_1, m_1) = (m_2x_1 + m_1x_2, m_1) = 1.$$

同理，$(x_2, m_2) = 1$. 结论成立.

从定理 **2.2.10** 我们可以推出欧拉函数 φ 的性质（即 φ 是所谓的乘性函数）.

定理 2.2.11 设 m，n 是互素的两个正整数. 则 $\varphi(mn) = \varphi(m)\varphi(n)$

证 根据定理 2.2.10，当 x 遍历模 m 的简化剩余系，共 $\varphi(m)$ 个整数，

以及 y 遍历模 n 的简化剩余系. 共 $\varphi(n)$ 个整数时，

$ym+xn$ 遍历 mn 的简化剩余系，其整数个数为 $\varphi(m)\varphi(n)$.

但模 mn 的简化剩余系的元素个数又为 $\varphi(mn)$，

因此，所以 $\varphi(mn)=\varphi(m)\varphi(n)$.

例 2.2.13 $\varphi(143) = \varphi(11)\varphi(13) = 10\cdot 12 = 120.$

$\varphi(105) = \varphi(3)\varphi(5)\varphi(7) = 2\cdot 4\cdot 6 = 48.$

下面给出欧拉函数的计算公式.

定理 2.2.12 设正整数 n 有标准因数分解式为 $n=\prod_{p|n} p^{\alpha} = p_1^{\alpha_1}\cdots p_k^{\alpha_s}$，

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

证 根据欧拉函数的可乘性，我们有

$$\begin{aligned}\varphi(n)&=\prod_{p|n}\varphi(p^{\alpha})\\&=\prod_{p|n}(p^{\alpha}-p^{\alpha-1})\\&=n(1-\frac{1}{p_1})\cdots(1-\frac{1}{p_k})\end{aligned}.$$

注 1： 设 p，q 是不同的素数，则 $\varphi(pq)=pq-p-q+1$.

注 2： 当 n 为合数，且不知道 n 的因数分解式时，通常很难求出 n 的欧拉函数值 $\varphi(n)$.

例 2.2.14 设正整数 n 是两个不同素数的乘积. 如果知道 n 和欧拉函数值 $\varphi(n)$，则可求出 n 的因数分解式.

证 考虑未知数 p，q 的方程组：

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

根据多项式的根与系数之间的关系，我们可以从二次方程

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

求出 n 的因数 p，q.

2.2.4 欧拉定理、费马小定理及 Wilson 定理

在实际应用中，经常要考虑模幂运算，即 $a^k \pmod m$. 为此，本节我们先学习三个重要的定理.

例 2.2.15 设 m=7，a=2，我们有 $(2,7)=1,\ \varphi(7)=6$.

考虑模 7 的最小非负简化剩余系 $x=$ 1，2，3，4，5，6，我们有 $2x=$

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

上述式子左右对应相乘，得到

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

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

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

故 $2^6\equiv 1 \pmod 7$.

例 2.2.16 设 m=30，a=7，我们有 $(7,30)=1,\ \varphi(30)=8$.

考虑模 30 的最小非负简化剩余系 x=1，7，11，13，17，19，23，29，我们有 $7x=$

$$7\cdot 1\equiv 7,\qquad 7\cdot 7\equiv 49\equiv 19,\qquad 7\cdot 11=77\equiv 17,$$
$$7\cdot 13=91\equiv 1,\qquad 7\cdot 17=119\equiv 29,\qquad 7\cdot 19=133\equiv 13,$$
$$7\cdot 23=161\equiv 11,\quad 7\cdot 29=203\equiv 23\ (\mathrm{mod}\,30)$$

上述式子左右对应相乘，得到

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

或 $7^8\cdot 1\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\equiv 1\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29\ (\mathrm{mod}\,30)$.

注意到 $(1\cdot 7\cdot 11\cdot 13\cdot 17\cdot 19\cdot 23\cdot 29,\ 30)=1,$

故 $7^8\equiv 1 \pmod{30}$.

如上例题可推广为一般的结论，即欧拉（*Euler*）定理.

定理 2.2.13（**欧拉定理**） 设 m 是大于 1 的整数，如果 a 是满足（a，m）=1 的整数，则 $a^{\varphi(m)}\equiv 1\ (\mathrm{mod}\,m)$.

证 取 $r_1,\cdots,r_{\varphi(m)}$ 为模 m 的一个最小正简化剩余系，

则当 a 是满足（a，m）=1 的整数时，根据定理 2.2.8 $ar_1,\cdots,ar_{\varphi(m)}$ 也为模 m 的一

个简化剩余系，这就是说，$ar_1,\cdots,ar_{\varphi(m)}$ 模 m 的最小正剩余是 $r_1,\cdots,r_{\varphi(m)}$ 的一个排列.

故 $(ar_1)\cdots(ar_{\varphi(m)})$ 模 m 的最小正剩余和乘积 $r_1,\cdots,r_{\varphi(m)}$ 模 m 的最小正剩余相等.

根据定理 2.1.2，我们有 $(ar_1)\cdots(ar_{\varphi(m)})\equiv r_1\cdots r_{\varphi(m)}\pmod m$.

因此，$r_1,\cdots,r_{\varphi(m)}(a^{\varphi(m)}-1)\equiv 0\pmod m$.

又从 $(r_1,m)=1,\cdots,(r_{\varphi(m)},m)=1$ 及推论 1.2.1，可推出 $(r_1\cdots r_{\varphi(m)},m)=1$.

从而，根据性质 2.1.3，得到 $a^{\varphi(m)}-1\equiv 0\pmod m$.

例 2.2.17 设 m=19，a=3，我们有（3，19）=1，$\varphi(19)=18$，故 $3^{18}\equiv 1\pmod{19}$.

设 m= 31，$a=2$，我们有（2，31）=1，$\varphi(31)=30$，故 $2^{30}\equiv 1\pmod{31}$.

在应用欧拉定理时，当 m 是素数时，给出费马（*Fermat*）小定理与 Wilson 定理.

定理 2.2.14 (费马小定理) 设 p 是一个素数，则对任意整数 a，我们有 $a^p\equiv a\pmod p$.

证 我们分两种情形考虑.

（*i*）若 a 被 p 整除，则同时 $a\equiv 0\pmod p$ 和 $a^p\equiv 0\pmod p$.

因此，由传递性 $a^p\equiv a\pmod p$.

（*ii*）若 a 不被 p 整除，则 (a,p)=1（见例 1.2.5）. 根据定理 2.2.13，$a^{p-1}\equiv 1\pmod p$.

两端同乘 a，得到 $a^p\equiv a\pmod p$.

例 2.2.18 应用欧拉定理可以证明 RSA 公钥密码算法的正确性. Ron Rivest 和 Adi Shamir 以及 Leonard Adleman 于 1978 年提出的 RSA 公钥密码体制至今仍被公认为是一个安全性能良好的密码体制. RSA 公钥密码体制的描述如下：

1) 选取两个大素数 p，q.
2) 计算 $n=pq$，$\phi(n)=(p-1)(q-1)$.
3) 随机选取正整数 e，$1<e<\phi(n)$，满足 $(e,\ \phi(n))=1$.
4) 计算 d，满足 $de\equiv 1(\mathrm{mod}\,\phi(n))$.

p，q，$\phi(n)$，d 是保密的；n，e 是公开的.

5) 加密变换：对明文 m，$1<m<n$，加密后的密文为 $c\equiv m^e\pmod n$.
6) 解密变换：对密文 c，$1<c<n$，解密后的明文 $m=c^d\pmod{\mathrm{n}}$.

这个解密变换能正确解出明文.

证 由于 $de \equiv 1(\bmod \phi(n))$，所以存在正整数 t，使得 $de \equiv 1+t\phi(n)$.

对任意明文 m，$1<m<n$,

当 $(m,n)=1$ 时，根据欧拉定理得

$$c^d \equiv (m^e)^d \equiv (m^{\phi(n)})^t m \equiv 1^t m \equiv m(\bmod n)\text{；} \quad \cdots\cdots\cdots\cdots\cdots (2.2.2)$$

当 $(m,n)\neq 1$ 时，因为 $n=pq$ 且 p，q 是两个素数，

所以 $\phi(n)=(p-1)(q-1)$；$(m,n)=p$ 或 q.

不妨设 $(m,n)=p$，则 $p \mid m$，设 $m=bp,\ 1\le b<q$.

另一方面，由欧拉定理得 $m^{q-1}=1(\bmod q)$，

从而 $m^{t\phi(n)}=(m^{q-1})^{t(p-1)} \equiv 1(\bmod q)$，于是存在一个整数 s，使得 $m^{t\phi(n)}=1+sq$，

此式两端用 $m=bp$ 同乘，就得到

$$m^{t\phi(n)+1}=m+bsn\text{，} \quad \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (2.2.3)$$

从而由（2.2.2）与（2.2.3）有，$c^d \equiv m^{t\phi(n)+1} \equiv m \pmod n$.

定理 2.2.15 （***Wilson* 定理**） 设 p 是一个素数. 则 $(p-1)!\equiv -1(\bmod p)$.

证 若 $p=2$，结论显然成立.

设 $p\ge 3$. 根据定理 2.2.9，对于每个整数 a，$1\le a\le p-1$，

存在惟一的整数 a'，$1\le a'\le p-1$，使得 $aa'\equiv 1(\bmod p)$.

又 $a=a'$ 的充要条件是 a 满足，$a^2\equiv 1(\bmod p)$.

这时，$a=1$ 或 $a=p-1$.

将 2，…，$p-2$ 中的 a 与 a' 配对，得到

$$\begin{aligned} 1\cdot 2\cdots(p-2)(p-1) &\equiv 1\cdot(p-1)\prod_a aa' \\ &\equiv 1\cdot(p-1) \\ &\equiv -1 \quad (\bmod p) \end{aligned}.$$

因此，结论成立.

例 2.2.19 设 $p=13$，我们有

$2\cdot 7 = 14 \equiv 1$，　$3\cdot 9 = 27 \equiv 1$，　$4\cdot 10 = 40 \equiv 1$，

$5\cdot 8 = 40 \equiv 1$，　$6\cdot 11 = 66 \equiv 1$，　$1\cdot 12 \equiv -1 \pmod{13}$,

因此，

1·2·3·4·5·6·7·8·9·10·11

= (1·12)(2·7)(3·9)(4·10)(5·8)(6·11)

≡ (-1)·1·1·1·1·1

≡ -1 (mod 13).

2.3 模重复平方计算法

对大整数模 m 和大整数 n，在进行 $b^n \pmod m$ 模幂运算时，

我们可以递归的计算

$$b^n \equiv (b^{n-1} \pmod m) \cdot b \pmod m .$$

但这种计算较为费时，须作 n-1 次乘法.

现在，将 n 写成二进制：$n = n_0 + n_1 2 + \cdots + n_{k-1} 2^{k-1}$，

其中 $n_i \in \{0,1\}$，i=0，1，…，k-1，则

$b^n \pmod m$ 的计算可归纳为:

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

我们最多作 $2[\log_2^n]$ 次乘法. 这个计算方法叫做“模重复平方计算法”.

“**模重复平方计算法**”具体算法如下：

（0）令 a=1，将 n 写成二进制：$n = n_0 + n_1 2 + \cdots + n_{k-1} 2^{k-1}$，其中 $n_i \in \{0,1\}$，i=0，1，…，k-1.

（1）如果 $n_0 = 1$，则计算 $a_0 \equiv a \cdot b \pmod m$，否则取 $a_0 = a$，即计算 $a_0 \equiv a \cdot b^{n_0} \pmod m$，再计算 $b_1 \equiv b^2 \pmod m$.

（2）如果 $n_1 = 1$，则计算 $a_1 \equiv a_0 \cdot b_1 \pmod m$，否则取 $a_1 = a_0$，即计算 $a_1 \equiv a_0 \cdot b_1^{n_1} \pmod m$，再计算 $b_2 \equiv b_1^2 \pmod m$.

……

（k-1）如果 $n_{k-2} = 1$，则计算 $a_{k-2} \equiv a_{k-3} \cdot b_{k-2} \pmod m$，否则取 $a_{k-2} = a_{k-3}$，即计算

$a_{k-2} \equiv a_{k-3} \cdot b_{k-2}^{n_{k-2}} \pmod{m}$，再计算 $b_{k-1} \equiv b_{k-2}^2 \pmod{m}$.

（k）如果 $n_{k-1}=1$，则计算 $a_{k-1} \equiv a_{k-2} \cdot b_{k-1} \pmod{m}$，否则取 $a_{k-1}=a_{k-2}$，即计算

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

最后，a_{k-1}就是 $b^n \pmod{m}$.

例 2.3.1 计算 $7^{29} \pmod{31}$.

解 设 m=31，b=7，令 a=1，将 29 写成二进制: $29 = 1+2^2+2^3+2^4 = (11101)_2$.

运用模重复平方计算法，我们依次计算如下:

（1）$n_0 = 1$，计算 $a_0 = a \cdot b \equiv 7$, $b_1 = b^2 \equiv 18 \pmod{31}$.

（2）$n_1 = 0$，计算 $a_1 = a_0 \equiv 7$, $b_2 = b_1^2 \equiv 14 \pmod{31}$.

（3）$n_2 = 1$，计算 $a_2 = a_1 \cdot b_2 \equiv 5$, $b_3 = b_2^2 \equiv 10 \pmod{31}$.

（4）$n_3 = 1$，计算 $a_3 = a_2 \cdot b_3 \equiv 19$, $b_4 = b_3^2 \equiv 7 \pmod{31}$.

（5）$n_4 = 1$，计算 $a_4 = a_3 \cdot b_4 \equiv 9 \pmod{31}$.

最后，计算得出 $7^{29} \equiv 9 \pmod{31}$.

例 2.3.2 计算 $32760^{365} \pmod{65521}$.

解 设 m=65521，b=32760，令 a=1，将 365 写成二进制: $365 = 1+2^2+2^3+2^5+2^6+2^8 = (101101101)_2$.

运用模重复平方计算法，我们依次计算如下:

（1）$n_0 = 1$，计算 $a_0 = a \cdot b \equiv 32760$, $b_1 = b^2 \equiv 49141 \pmod{65521}$.

（2）$n_1 = 0$，计算 $a_1 = a_0 \equiv 32760$, $b_2 = b_1^2 \equiv 61426 \pmod{65521}$.

（3）$n_2 = 1$，计算 $a_2 = a_1 \cdot b_2 \equiv 34808$, $b_3 = b_2^2 \equiv 61170 \pmod{65521}$.

（4）$n_3 = 1$，计算 $a_3 = a_2 \cdot b_3 \equiv 34944$, $b_4 = b_3^2 \equiv 61153 \pmod{65521}$.

（5）$n_4 = 0$，计算 $a_4 = a_3 \equiv 34944$, $b_5 = b_4^2 \equiv 12813 \pmod{65521}$.

（6）$n_5 = 1$，计算 $a_5 = a_4 \cdot b_5 \equiv 32479$, $b_6 = b_5^2 \equiv 42864 \pmod{65521}$.

（7）$n_6 = 1$，计算 $a_6 = a_5 \cdot b_6 \equiv 55169$, $b_7 = b_6^2 \equiv 48135 \pmod{65521}$.

（8）$n_7 = 0$，计算 $a_7 = a_6 \equiv 55169$, $b_8 = b_7^2 \equiv 24623 \pmod{65521}$.

（9）$n_8 = 1$，计算 $a_8 = a_7 \cdot b_8 \equiv 44915 \pmod{65521}$.

最后，计算得出 $32760^{365} \equiv 44915 \pmod{65521}$.