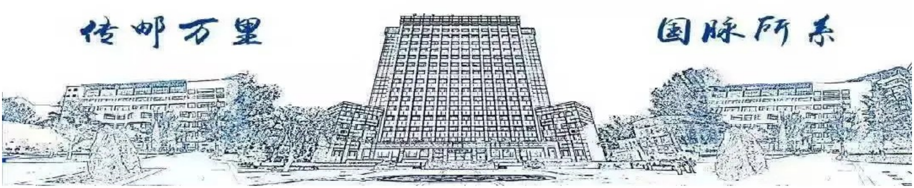
网络空间安全学院
School of Cyberspace Security, BUPT

信息安全数学基础

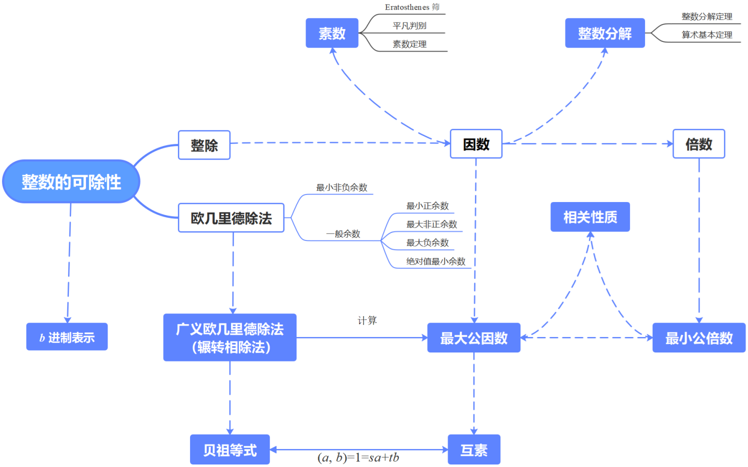
—— 同余 (1)

信数课题组

北京邮电大学



上次课回顾



Eratosthenes 筛
素数
平凡判别
素数定理
整数分解
整数分解定理
算术基本定理
整除
因数
倍数
整数的可除性
欧几里德除法
最小非负余数
一般余数
最小正余数
最大非正余数
最大负余数
绝对值最小余数
相关性质
b 进制表示
广义欧几里德除法（辗转相除法）
计算
最大公因数
最小公倍数
贝祖等式
互素
(a, b)=1=sa+tb

目录

1 同余的概念及基本性质
- 同余的概念
- 同余的基本性质

2 剩余类
- 剩余及剩余类
- 完全剩余系

目录

1. 同余的概念及基本性质
   - 同余的概念
   - 同余的基本性质
2. 剩余类
   - 剩余及剩余类
   - 完全剩余系

定义 2.1.1

给定一个正整数 m, 设 a, b 是两个整数. 若 $a-b$ 被 m 整除, 或 $m \mid a-b$, 则称 a, b **模 m 同余**, 记作 $a \equiv b \bmod m$. 否则, 称 a, b **模 m 不同余**, 记作 $a \not\equiv b \bmod m$.

定义 2.1.1

给定一个正整数 m, 设 a, b 是两个整数. 若 $a-b$ 被 m 整除, 或 $m \mid a-b$, 则称 a, b **模 m 同余**, 记作 $a \equiv b \bmod m$. 否则, 称 a, b **模 m 不同余**, 记作 $a \not\equiv b \bmod m$.

注 1: 同余是数论中的一个十分重要的概念, 也常常出现于日常生活中. 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.

定义 2.1.1

给定一个正整数 m, 设 a, b 是两个整数. 若 $a-b$ 被 m 整除, 或 $m \mid a-b$, 则称 a, b **模 m 同余**, 记作 $a \equiv b \bmod m$. 否则, 称 a, b **模 m 不同余**, 记作 $a \not\equiv b \bmod m$.

注 1: 同余是数论中的一个十分重要的概念, 也常常出现于日常生活中. 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.

注: 最先引用同余概念与 $\equiv$ 符号者是 Gauss (高斯).

定义 2.1.1

给定一个正整数 m, 设 a, b 是两个整数. 若 $a-b$ 被 m 整除, 或 $m \mid a-b$, 则称 a, b **模 m 同余**, 记作 $a \equiv b \bmod m$. 否则, 称 a, b **模 m 不同余**, 记作 $a \not\equiv b \bmod m$.

注 1: 同余是数论中的一个十分重要的概念, 也常常出现于日常生活中. 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.

注: 最先引用同余概念与 $\equiv$ 符号者是 Gauss (高斯).

约翰・卡尔・弗里德里希・高斯

(Johann Carl Friedrich Gauss, 1777.4.30 — 1855.2.23)

德国数学家、物理学家、天文学家、大地测量学家，近代数学奠基者之一. 17 岁发现了素数分布定理和最小二乘法, 成功得到后人熟知的正态分布 (高斯分布). 次年, 证明出仅用尺规便可以构造出 17 边形. 在著作《算术研究》中, 证明了二次互反律, 成为数论继续发展的重要基础. 因其卓越的数学成就, 被认为是世界上最重要的数学家之一, 并享有“数学王子”的美誉.

例 2.1.1 (1) $100 \equiv 2 \mod 7$, 因为 $7 \mid 100 - 2$.

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

例 2.1.1 (1) $100 \equiv 2 \mod 7$, 因为 $7 \mid 100 - 2$.

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

如何判断两个整数 a, b 模 m 同余呢?

定理 2.1.1

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

例 2.1.1 (1) $100 \equiv 2 \mod 7$, 因为 $7 \mid 100 - 2$.

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

如何判断两个整数 a, b 模 m 同余呢?

定理 2.1.1

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

证: 如果 $a \equiv b \mod m$, 根据同余的定义有 $m \mid a - b$. 又根据整除的定义, 存在一个整数 k 使得 $a - b = k \cdot m$, 即 $a = b + k \cdot m$.

反过来, 如果存在一个整数 k 使得 $a = b + k \cdot m$, 则有 $a - b = k \cdot m$. 根据整除的定义有, $m \mid a - b$. 再根据同余的定义知, $a \equiv b \mod m$.

例 2.1.1 (1) $100 \equiv 2 \mod 7$, 因为 $7 \mid 100 - 2$.

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

如何判断两个整数 a, b 模 m 同余呢？

定理 2.1.1

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

证：如果 $a \equiv b \mod m$, 根据同余的定义有 $m \mid a - b$. 又根据整除的定义, 存在一个整数 k 使得 $a - b = k \cdot m$, 即 $a = b + k \cdot m$.

反过来, 如果存在一个整数 k 使得 $a = b + k \cdot m$, 则有 $a - b = k \cdot m$. 根据整除的定义有, $m \mid a - b$. 再根据同余的定义知, $a \equiv b \mod m$.

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

定理 2.1.2

设 m 是一个正整数，则整数 $a \equiv b \mod m$ 的充要条件是 a, b 被 m 除的余数相同.

定理 2.1.2

设 m 是一个正整数，则整数 $a \equiv b \mod m$ 的充要条件是 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

$$a = q \cdot m + r, 0 \leqslant r < m; \ b = q' \cdot m + r', 0 \leqslant r' < m.$$

两式相减，得到 $a - b = (q - q') \cdot m + (r - r')$,

或者 $$(r - r') = (a - b) - (q - q') \cdot m.$$

因此，$m \mid a - b$ 的充要条件是 $m \mid r - r'$.

但因为 $0 \leqslant |r - r'| < m$，则 $m \mid r - r'$ 的充要条件是 $r - r' = 0$,

所以 $m \mid a - b$ 的充要条件是 $r - r' = 0$.

定理 2.1.2

设 m 是一个正整数, 则整数 $a \equiv b \mod m$ 的充要条件是 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

$$a = q \cdot m + r, 0 \leqslant r < m; \;\; b = q' \cdot m + r', 0 \leqslant r' < m.$$

两式相减, 得到 $a - b = (q - q') \cdot m + (r - r')$,

或者 $\qquad (r - r') = (a - b) - (q - q') \cdot m.$

因此, $m \mid a - b$ 的充要条件是 $m \mid r - r'$.

但因为 $0 \leqslant |r - r'| < m$, 则 $m \mid r - r'$ 的充要条件是 $r - r' = 0$,

所以 $m \mid a - b$ 的充要条件是 $r - r' = 0$.

例 2.1.3 $\quad 2024 \equiv 1485 \mod 7$,

因为 $2024 = 289 \cdot 7 + 1$, $1485 = 212 \cdot 7 + 1$.

例 2.1.4 单表密码.

例 2.1.4 单表密码.

表 2.1 英文字母和模 26 的剩余之间的对应关系.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

例 2.1.4 单表密码.

表 2.1 英文字母和模 26 的剩余之间的对应关系.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
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, 便可以将 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对应的字母. 用公式表达为 $E \equiv P + 3 \mod 26$, 其中 P 为明文字母对应的数字, E 为密文字母对应的数字.

例 2.1.4 单表密码.

表 2.1 英文字母和模 26 的剩余之间的对应关系.

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12
n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

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. 如当 $k=7, b=6$ 时, 便可以将 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.

目录

1. 同余的概念及基本性质
   - 同余的概念
   - 同余的基本性质
2. 剩余类
   - 剩余及剩余类
   - 完全剩余系

性质 2.1.1

设 m 是一个正整数，则模 m 同余是**等价关系**，即

(1) (自反性) 对任意整数 a，有 $a \equiv a \mod m$.

(2) (对称性) 若 $a \equiv b \mod m$，则 $b \equiv a \mod m$.

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

性质 2.1.1

设 m 是一个正整数, 则模 m 同余是**等价关系**, 即

(1) (自反性) 对任意整数 a, 有 $a \equiv a \mod m$.

(2) (对称性) 若 $a \equiv b \mod m$, 则 $b \equiv a \mod m$.

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

证：(1) (自反性) 对任意整数 a, 有 $a = a + 0 \cdot m$, 所以 $a \equiv a \mod m$.

性质 2.1.1

设 m 是一个正整数, 则模 m 同余是**等价关系**, 即

(1) (自反性) 对任意整数 a, 有 $a \equiv a \mod m$.

(2) (对称性) 若 $a \equiv b \mod m$, 则 $b \equiv a \mod m$.

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

证：(1) (自反性) 对任意整数 a, 有 $a = a + 0 \cdot m$, 所以 $a \equiv a \mod m$.

(2) (对称性) 若 $a \equiv b \mod m$, 则存在整数 k 使得 $a = b + k \cdot m$, 从而有 $b = a + (-k) \cdot m$. 因此, $b \equiv a \mod m$.

性质 2.1.1

设 m 是一个正整数, 则模 m 同余是**等价关系**, 即

(1) (自反性) 对任意整数 a, 有 $a \equiv a \mod m$.

(2) (对称性) 若 $a \equiv b \mod m$, 则 $b \equiv a \mod m$.

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

证：(1) (自反性) 对任意整数 a, 有 $a = a + 0 \cdot m$, 所以 $a \equiv a \mod m$.

(2) (对称性) 若 $a \equiv b \mod m$, 则存在整数 k 使得 $a = b + k \cdot m$, 从而有 $b = a + (-k) \cdot m$. 因此, $b \equiv a \mod m$.

(3) (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 $a = b + k_1 \cdot m$, $b = c + k_2 \cdot m$, 从而 $a = c + (k_1 + k_2) \cdot m$. 因为 $k_1 + k_2$ 是整数, 所以 $a \equiv c \mod m$.

性质 2.1.2

设 m 是一个正整数，设 a_1, a_2, b_1, b_2 是四个整数，如果 $a_1 \equiv b_1 \mod m$，$a_2 \equiv b_2 \mod m$，则

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

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

性质 2.1.2

设 m 是一个正整数，设 a_1, a_2, b_1, b_2 是四个整数，如果 $a_1 \equiv b_1 \mod m$，$a_2 \equiv b_2 \mod m$，则

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

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

证：依题设，根据定理 2.1.1，分别存在整数 k_1, k_2 使得 $a_1 = b_1 + k_1 \cdot m$，$a_2 = b_2 + k_2 \cdot m$，从而

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

$$\begin{aligned} a_1 \cdot a_2 &= b_1 \cdot b_2 + (k_1 \cdot m) \cdot b_2 + b_1 \cdot (k_2 \cdot m) + (k_1 \cdot m)(k_2 \cdot m) \\ &= b_1 \cdot b_2 + (k_1 \cdot b_2 + b_1 \cdot k_2 + k_1 \cdot k_2 \cdot m) \cdot m. \end{aligned}$$

因为 $k_1 + k_2, k_1 \cdot b_2 + b_1 \cdot k_2 + k_1 \cdot k_2 \cdot m$ 都是整数，所以根据定理 2.1.1 知，$a_1 + a_2 \equiv b_1 + b_2 \mod m$，$a_1 \cdot a_2 \equiv b_1 \cdot b_2 \mod m$.

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

$$2024 \equiv 715 \mod 7. \qquad \text{传递性}$$

同时, 我们有

$$2024 \equiv 2024 \mod 7,\ 1485 \equiv 1485 \mod 7,\ 715 \equiv 715 \mod 7. \qquad \text{自反性}$$

以及

$$1485 \equiv 2024 \mod 7,\ 715 \equiv 1485 \mod 7. \qquad \text{对称性}$$

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

$$2024 \equiv 715 \mod 7. \qquad \text{传递性}$$

同时, 我们有

$$2024 \equiv 2024 \mod 7,\ 1485 \equiv 1485 \mod 7,\ 715 \equiv 715 \mod 7. \qquad \text{自反性}$$

以及

$$1485 \equiv 2024 \mod 7,\ 715 \equiv 1485 \mod 7. \qquad \text{对称性}$$

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

$$\begin{aligned}
3024 &= 2024 + 1000 \equiv 1 + (-1) \equiv 0 \mod 7,\\
1024 &= 2024 - 1000 \equiv 1 - (-1) \equiv 2 \mod 7,\\
2024000 &= 2024 \cdot 1000 \equiv 1 \cdot (-1) \equiv -1 \mod 7,\\
4096576 &= 2024^2 \equiv 1^2 \equiv 1 \mod 7,\\
1000000 &= 1000^2 \equiv (-1)^2 \equiv 1 \mod 7.
\end{aligned}$$

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

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 2^{2024} 天后是星期四.

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 2^{2024} 天后是星期四.

推论 2.1.1

若 $x \equiv y \mod m, a_i \equiv b_i \mod m, 0 \leqslant i \leqslant k$, 则

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

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 2^{2024} 天后是星期四.

推论 2.1.1

若 $x \equiv y \mod m, a_i \equiv b_i \mod m, 0 \leqslant i \leqslant k$, 则

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

证：由 $x \equiv y \mod m$, 根据性质 2.1.2, 有 $x^i \equiv y^i \mod m, 0 \leqslant i \leqslant k$.

又 $a_i \equiv b_i \mod m, 0 \leqslant i \leqslant k$, 将它们对应相乘, 得

$$a_i x^i \equiv b_i y^i \mod m, 0 \leqslant i \leqslant k.$$

最后, 将这些式子左右对应相加, 得到

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

推论 2.1.2

设整数 n 有十进制表示式

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

则 (i) $3 \mid n$ 的充要条件是

$$3 \mid a_k + \cdots + a_0.$$

(ii) $9 \mid n$ 的充要条件是

$$9 \mid a_k + \cdots + a_0.$$

推论 2.1.2

设整数 n 有十进制表示式

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

则 (i) $3 \mid n$ 的充要条件是

$$3 \mid a_k + \cdots + a_0.$$

(ii) $9 \mid n$ 的充要条件是

$$9 \mid a_k + \cdots + a_0.$$

证：因为 $10 \equiv 1 \mod 3$, 又 $1^i = 1, 0 \leqslant i \leqslant k$, 根据推论 2.1.1, 有

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

因此,

$$a_k 10^k + a_{k-1} 10^{k-1} + \cdots + a_1 10 + a_0 \equiv 0 \mod 3$$

的充要条件是

$$a_k + \cdots + a_0 \equiv 0 \mod 3.$$

即结论 (i) 成立.

同理, 结论 (ii) 也成立.

推论 2.1.3

设整数 n 有一千进制表示式

$$n = a_k 1000^k + \cdots + a_1 1000 + a_0, 0 \leqslant a_i \leqslant 1000.$$

则 7 (或 11, 或 13) 整除 n 的充要条件是 7 (或 11, 或 13) 整除整数

$$(a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots).$$

推论 2.1.3

设整数 n 有一千进制表示式

$$n = a_k 1000^k + \cdots + a_1 1000 + a_0, 0 \leqslant a_i \leqslant 1000.$$

则 7 (或 11, 或 13) 整除 n 的充要条件是 7 (或 11, 或 13) 整除整数

$$(a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots).$$

证：因为 $1000 = 7 \cdot 11 \cdot 13 - 1 \equiv -1 \mod 7$, 所以有

$$1000 \equiv 1000^3 \equiv 1000^5 \equiv \cdots \equiv -1 \mod 7.$$

$$1000^2 \equiv 1000^4 \equiv 1000^6 \equiv \cdots \equiv 1 \mod 7.$$

根据推论 2.1.1, 可立即得到

$$\begin{aligned} & a_k 1000^k + a_{k-1} 1000^{k-1} + \cdots + a_1 1000 + a_0 \\ \equiv\ & a_k(-1)^k + a_{k-1}(-1)^{k-1} + \cdots + a_1(-1) + a_0 \\ \equiv\ & (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots) \mod 7. \end{aligned}$$

因此, $m = 7$ 整除 n 的充要条件是 $7 \mid (a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots)$.

同理, 结论对于 $m = 11$ 或 13 也成立.

例 2.1.8 设 $n = 20240901$, 则 $3 \mid n$, $9 \mid n$.

解：因为 $a_k + \cdots + a_0 = 2 + 2 + 4 + 9 + 1 = 18$.

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

例 2.1.8 设 $n = 20240901$, 则 $3 \mid n$, $9 \mid n$.

解：因为 $a_k + \cdots + a_0 = 2 + 2 + 4 + 9 + 1 = 18$.

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

例 2.1.9 设 $n = 20240922$, 则 n 被 3 整除, 但不能被 9 整除.

解：因为 $a_k + \cdots + a_0 = 2 + 2 + 4 + 9 + 2 + 2 = 21 = 3 \cdot 7$.

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

例 2.1.8 设 $n = 20240901$, 则 $3 \mid n$, $9 \mid n$.

解：因为 $a_k + \cdots + a_0 = 2 + 2 + 4 + 9 + 1 = 18$.

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

例 2.1.9 设 $n = 20240922$, 则 n 被 3 整除, 但不能被 9 整除.

解：因为 $a_k + \cdots + a_0 = 2 + 2 + 4 + 9 + 2 + 2 = 21 = 3 \cdot 7$.

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

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

解：因为 $n = 20 \cdot 1000^2 + 240 \cdot 1000 + 920$, 又 $(a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots) = 920 + 20 - 240 = 700 = 2^2 \cdot 5^2 \cdot 7$, 所以 $7 \mid n$, $11 \nmid n$, $13 \nmid n$.

例 2.1.8 设 $n = 20240901$, 则 $3 \mid n$, $9 \mid n$.

解：因为 $a_k + \cdots + a_0 = 2 + 2 + 4 + 9 + 1 = 18$.

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

例 2.1.9 设 $n = 20240922$, 则 n 被 3 整除, 但不能被 9 整除.

解：因为 $a_k + \cdots + a_0 = 2 + 2 + 4 + 9 + 2 + 2 = 21 = 3 \cdot 7$.

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

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

解：因为 $n = 20 \cdot 1000^2 + 240 \cdot 1000 + 920$, 又 $(a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots) = 920 + 20 - 240 = 700 = 2^2 \cdot 5^2 \cdot 7$, 所以 $7 \mid n$, $11 \nmid n$, $13 \nmid n$.

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

解：因为 $n = 20 \cdot 1000^2 + 240 \cdot 1000 + 922$, 又 $(a_0 + a_2 + \cdots) - (a_1 + a_3 + \cdots) = 922 + 20 - 240 = 702 = 2 \cdot 3^3 \cdot 13$, 所以 $13 \mid n$, $7 \nmid n$, $11 \nmid n$.

性质 2.1.3

设 m 是一个正整数，设 $d \cdot a \equiv d \cdot b \mod m$. 如果 $(d, m) = 1$，则

$$a \equiv b \mod m.$$

性质 2.1.3

设 m 是一个正整数，设 $d \cdot a \equiv d \cdot b \mod m$. 如果 $(d, m) = 1$, 则

$$a \equiv b \mod m.$$

证：由 $d \cdot a \equiv d \cdot b \mod m$ 知, $m \mid d \cdot a - d \cdot b$, 即 $m \mid d \cdot (a - b)$.
因为 $(d, m) = 1$, 根据定理 1.2.8, 我们有 $m \mid a - b$, 故结论成立.

性质 2.1.3

设 m 是一个正整数，设 $d \cdot a \equiv d \cdot b \mod m$. 如果 $(d, m) = 1$，则

$$a \equiv b \mod m.$$

证：由 $d \cdot a \equiv d \cdot b \mod m$ 知，$m \mid d \cdot a - d \cdot b$，即 $m \mid d \cdot (a - b)$. 因为 $(d, m) = 1$，根据定理 1.2.8，我们有 $m \mid a - b$，故结论成立.

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

性质 2.1.3

设 m 是一个正整数，设 $d \cdot a \equiv d \cdot b \pmod{m}$. 如果 $(d, m) = 1$, 则

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

证：由 $d \cdot a \equiv d \cdot b \pmod{m}$ 知，$m \mid d \cdot a - d \cdot b$, 即 $m \mid d \cdot (a - b)$.
因为 $(d, m) = 1$, 根据定理 1.2.8, 我们有 $m \mid a - b$, 故结论成立.

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

性质 2.1.4

设 m 是一个正整数，如果 $a \equiv b \pmod{m}$, $k > 0$, 则

$$k \cdot a \equiv k \cdot b \pmod{(k \cdot m)}.$$

性质 2.1.3

设 m 是一个正整数，设 $d \cdot a \equiv d \cdot b \mod m$. 如果 $(d, m) = 1$, 则

$$a \equiv b \mod m.$$

证：由 $d \cdot a \equiv d \cdot b \mod m$ 知，$m \mid d \cdot a - d \cdot b$, 即 $m \mid d \cdot (a - b)$. 因为 $(d, m) = 1$, 根据定理 1.2.8, 我们有 $m \mid a - b$, 故结论成立.

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

性质 2.1.4

设 m 是一个正整数，如果 $a \equiv b \mod m$, $k > 0$, 则

$$k \cdot a \equiv k \cdot b \mod (k \cdot m).$$

证：由 $a \equiv b \mod m$, 根据定理 2.1.1, 存在整数 q 使得 $a = b + q \cdot m$. 进而，$k \cdot a = k \cdot b + q \cdot (k \cdot m)$. 因此，$k \cdot a \equiv k \cdot b \mod (k \cdot m)$.

性质 2.1.3

设 m 是一个正整数，设 $d \cdot a \equiv d \cdot b \mod m$. 如果 $(d, m) = 1$, 则

$$a \equiv b \mod m.$$

证：由 $d \cdot a \equiv d \cdot b \mod m$ 知, $m \mid d \cdot a - d \cdot b$, 即 $m \mid d \cdot (a - b)$. 因为 $(d, m) = 1$, 根据定理 1.2.8, 我们有 $m \mid a - b$, 故结论成立.

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

性质 2.1.4

设 m 是一个正整数，如果 $a \equiv b \mod m$, $k > 0$, 则

$$k \cdot a \equiv k \cdot b \mod (k \cdot m).$$

证：由 $a \equiv b \mod m$, 根据定理 2.1.1, 存在整数 q 使得 $a = b + q \cdot m$. 进而, $k \cdot a = k \cdot b + q \cdot (k \cdot m)$. 因此, $k \cdot a \equiv k \cdot b \mod (k \cdot m)$.

例 2.1.13 因为 $31 \equiv 3 \mod 7$, $k = 5 > 0$, 所以 $155 \equiv 15 \mod 35$.

性质 2.1.5

设 m 是一个正整数, $a \equiv b \mod m$, 如果整数 $d \mid (a,b,m)$, 则

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

性质 2.1.5

设 m 是一个正整数, $a \equiv b \mod m$, 如果整数 $d \mid (a,b,m)$, 则
$$\frac{a}{d} \equiv \frac{b}{d} \mod \frac{m}{d}.$$

证：因为 $d \mid (a,b,m)$, 所以存在整数 a', b', m' 使得
$$a = a' \cdot d, b = b' \cdot d, m = m' \cdot d.$$
而 $a \equiv b \mod m$, 所以存在整数 k 使得 $a = b + k \cdot m$, 即
$$a' \cdot d = b' \cdot d + k \cdot m' \cdot d.$$
又因 $d \mid (a,b,m)$, 则 $d \neq 0$, 故 $a' = b' + k \cdot m'$, 也就是
$$a' \equiv b' \mod m' \quad 或者 \quad \frac{a}{d} \equiv \frac{b}{d} \mod \frac{m}{d}.$$

性质 2.1.5

设 m 是一个正整数, $a \equiv b \mod m$, 如果整数 $d \mid (a, b, m)$, 则

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

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

$$a = a' \cdot d, b = b' \cdot d, m = m' \cdot d.$$

而 $a \equiv b \mod m$, 所以存在整数 k 使得 $a = b + k \cdot m$, 即

$$a' \cdot d = b' \cdot d + k \cdot m' \cdot d.$$

又因 $d \mid (a, b, m)$, 则 $d \neq 0$, 故 $a' = b' + k \cdot m'$, 也就是

$$a' \equiv b' \mod m' \quad \text{或者} \quad \frac{a}{d} \equiv \frac{b}{d} \mod \frac{m}{d}.$$

例 2.1.14　因为 $155 \equiv 15 \mod 35$, 所以取 $d = 5$, 得到 $31 \equiv 3 \mod 7$.

性质 2.1.6

设 m 是一个正整数, $a \equiv b \mod m$, 如果 $d \mid m$, 则 $a \equiv b \mod d$.

性质 2.1.6

设 m 是一个正整数, $a \equiv b \mod m$, 如果 $d \mid m$, 则 $a \equiv b \mod d$.

证：因为 $d \mid m$, 所以存在整数 m' 使得 $m = m' \cdot d$. 又因为 $a \equiv b \mod m$, 所以存在整数 k 使得 $a = b + k \cdot m$, 即 $a = b + (k \cdot m') \cdot d$.

故 $a \equiv b \mod d$.

性质 2.1.6

设 m 是一个正整数, $a \equiv b \mod m$, 如果 $d \mid m$, 则 $a \equiv b \mod d$.

证：因为 $d \mid m$, 所以存在整数 m' 使得 $m = m' \cdot d$. 又因为 $a \equiv b \mod m$, 所以存在整数 k 使得 $a = b + k \cdot m$, 即 $a = b + (k \cdot m') \cdot d$.

故 $a \equiv b \mod d$.

例 2.1.15 因为 $169 \equiv 29 \mod 35$, 所以取 $d = 7$, 得 $169 \equiv 29 \mod 7$.

性质 2.1.6

设 m 是一个正整数, $a \equiv b \mod m$, 如果 $d \mid m$, 则 $a \equiv b \mod d$.

证：因为 $d \mid m$, 所以存在整数 m' 使得 $m = m' \cdot d$. 又因为 $a \equiv b \mod m$, 所以存在整数 k 使得 $a = b + k \cdot m$, 即 $a = b + (k \cdot m') \cdot d$.

故 $a \equiv b \mod d$.

例 2.1.15 因为 $169 \equiv 29 \mod 35$, 所以取 $d = 7$, 得 $169 \equiv 29 \mod 7$.

性质 2.1.7

设 $m_1, \cdots, m_k$ 是 k 个正整数, $a \equiv b \mod m_i$, $i = 1, \cdots, k$, 则

$$a \equiv b \mod [m_1, \cdots, m_k].$$

性质 2.1.6

设 m 是一个正整数, $a \equiv b \mod m$, 如果 $d \mid m$, 则 $a \equiv b \mod d$.

证：因为 $d \mid m$, 所以存在整数 m' 使得 $m = m' \cdot d$. 又因为 $a \equiv b \mod m$, 所以存在整数 k 使得 $a = b + k \cdot m$, 即 $a = b + (k \cdot m') \cdot d$.

故 $a \equiv b \mod d$.

例 2.1.15 因为 $169 \equiv 29 \mod 35$, 所以取 $d = 7$, 得 $169 \equiv 29 \mod 7$.

性质 2.1.7

设 $m_1, \cdots, m_k$ 是 k 个正整数, $a \equiv b \mod m_i$, $i = 1, \cdots, k$, 则

$$a \equiv b \mod [m_1, \cdots, m_k].$$

证：由 $a \equiv b \mod m_i$, $i = 1, \cdots, k$ 知, $m_i \mid a - b$, $i = 1, \cdots, k$.
根据定理 1.2.14, 有 $[m_1, \cdots, m_k] \mid a - b$, 即 $a \equiv b \mod [m_1, \cdots, m_k]$.

例 2.1.16 因为 $155 \equiv 15 \mod 5$, $155 \equiv 15 \mod 7$, $(5,7) = 1$, $[5,7] = 35$, 所以 $155 \equiv 15 \mod 35$.

例 2.1.16　因为 $155 \equiv 15 \mod 5$, $155 \equiv 15 \mod 7$, $(5,7)=1$, $[5,7]=35$, 所以 $155 \equiv 15 \mod 35$.

性质 2.1.8

设 $a \equiv b \mod m$, 则 $(a,m)=(b,m)$.

例 2.1.16　因为 $155 \equiv 15 \mod 5$, $155 \equiv 15 \mod 7$, $(5,7)=1$, $[5,7]=35$, 所以 $155 \equiv 15 \mod 35$.

性质 2.1.8

设 $a \equiv b \mod m$, 则 $(a,m)=(b,m)$.

证：由 $a \equiv b \mod m$ 知, 存在整数 k 使得

$$a = b + k \cdot m.$$

根据定理 1.2.2, 有

$$(a,m) = (b,m).$$

目录

1 同余的概念及基本性质
- 同余的概念
- 同余的基本性质

2 剩余类
- 剩余及剩余类
- 完全剩余系

同余是一种等价关系, 因此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.

设 m 是一个正整数. 对任意整数 a, 令

$$C_a = \{c \in \mathbb{Z} \mid c \equiv a \mod m\}. \tag{2.2.1}$$

C_a 是非空集合, 因为 $a \in C_a$.

同余是一种等价关系, 因此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.

设 m 是一个正整数. 对任意整数 a, 令

$$C_a = \{c \in \mathbb{Z} \mid c \equiv a \pmod m\}. \tag{2.2.1}$$

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**).

同余是一种等价关系, 因此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.

设 m 是一个正整数. 对任意整数 a, 令

$$C_a = \{c \in \mathbb{Z} \mid c \equiv a \mod m\}. \tag{2.2.1}$$

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) 任一整数必包含再一个 C_r 中, $0 \leqslant r \leqslant m-1$.

(ii) $C_a = C_b$ 的充要条件是 $a \equiv b \mod m$.

(iii) C_a 与 C_b 的交集为空集的充要条件是 $a \not\equiv b \mod m$.

证：(i) 设 a 是任一整数, 根据欧几里德除法, 存在唯一的整数 q, r 使得 $a = q \cdot m + r,\ 0 \leqslant r < m$. 因此, 有 $a \equiv r \mod m, a$ 包含在 C_r 中.

证：(i) 设 a 是任一整数, 根据欧几里德除法, 存在唯一的整数 q, r 使得 $a = q \cdot m + r,\ 0 \leqslant r < m$. 因此, 有 $a \equiv r \mod m, a$ 包含在 C_r 中.

(ii) 因为 $b \in C_b = C_a$, 所以必要性成立.

证：(i) 设 a 是任一整数, 根据欧几里德除法, 存在唯一的整数 q, r 使得 $a = q \cdot m + r,\ 0 \leqslant r < m$. 因此, 有 $a \equiv r \mod m, a$ 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. 若 $a \equiv b \mod m$, 则对任意整数 $c \in C_a$, 即 $c \equiv a \mod m$, 由性质 2.1.1 (iii) (传递性) 得, $c \equiv b \mod m$, 即 $c \in C_b$, 故得 $C_a \subset C_b$. 同理, 可得 $C_b \subset C_a$. 故 $C_a = C_b$.

证：(i) 设 a 是任一整数, 根据欧几里德除法, 存在唯一的整数 q, r 使得 $a = q \cdot m + r,\ 0 \leqslant r < m$. 因此, 有 $a \equiv r \mod m, a$ 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. 若 $a \equiv b \mod m$, 则对任意整数 $c \in C_a$, 即 $c \equiv a \mod m$, 由性质 2.1.1 (iii) (传递性) 得, $c \equiv b \mod m$, 即 $c \in C_b$, 故得 $C_a \subset C_b$. 同理, 可得 $C_b \subset C_a$. 故 $C_a = C_b$.

(iii) 由（ii）立得必要性.

证：(i) 设 a 是任一整数, 根据欧几里德除法, 存在唯一的整数 q, r 使得 $a = q \cdot m + r,\ 0 \leqslant r < m$. 因此, 有 $a \equiv r \mod m, a$ 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. 若 $a \equiv b \mod m$, 则对任意整数 $c \in C_a$, 即 $c \equiv a \mod m$, 由性质 2.1.1 (iii) (传递性) 得, $c \equiv b \mod m$, 即 $c \in C_b$, 故得 $C_a \subset C_b$. 同理, 可得 $C_b \subset C_a$. 故 $C_a = C_b$.

(iii) 由（ii）立得必要性.

充分性 (反证法). 若 $a \not\equiv b \mod m$, 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

$$c \equiv a \mod m \quad 及 \quad c \equiv b \mod m.$$

对于 $c \equiv a \mod m$, 根据性质 2.1.1 (ii) (对称性) 知, $a \equiv c \mod m$. 再根据性质 2.1.1 (iii) (传递性) 及 $c \equiv b \mod m$ 得, $a \equiv b \mod m$. 这与假设矛盾, 故 C_a 与 C_b 的交集为空集.

目录

1 同余的概念及基本性质
- 同余的概念
- 同余的基本性质

2 剩余类
- 剩余及剩余类
- 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个剩余类里, 则 $r_0, r_1, \cdots, r_{m-1}$ 叫做模 m 的一个**完全剩余系**.

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个剩余类里，则 $r_0, r_1, \cdots, r_{m-1}$ 叫做模 m 的一个**完全剩余系**.

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

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个剩余类里，则 $r_0, r_1, \cdots, r_{m-1}$ 叫做模 m 的一个**完全剩余系**.

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

例 2.2.1　设正整数 $m = 12$. 对任意整数 a，集合 $C_a = \{a + 12k | k \in \mathbb{Z}\}$ 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要条件是它们模 m 两两不同余.

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**.

定义 2.2.3 (续)

(v) 当 m 为偶数时,

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

或

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

是模 m 的一个完全剩余系;

当 m 为奇数时,

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

是模 m 的一个完全剩余系.

上述两个完全剩余系统称为模 m 的一个**绝对值最小完全剩余系**.

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 遍历模 m 的一个完全剩余系, 则 $a\cdot x+b$ 也遍历模 m 的一个完全剩余系.

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 遍历模 m 的一个完全剩余系, 则 $a \cdot x + b$ 也遍历模 m 的一个完全剩余系.

证：根据定理 2.2.2, 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 $a \cdot a_0 + b, a \cdot a_1 + b, \cdots, a \cdot a_{m-1} + b$ 模 m 两两不同余.

事实上, 若存在 a_i 和 a_j $(i \neq j)$ 使得 $a \cdot a_i + b \equiv a \cdot a_j + b \mod m$, 则 $m \mid a \cdot (a_i - a_j)$. 因为 $(a, m) = 1$, 我们有 $m \mid a_i - a_j$, 这说明 a_i 和 a_j 模 m 同余, 与假设矛盾.

因此, $a \cdot x + b$ 也遍历模 m 的一个完全剩余系.

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 遍历模 m 的一个完全剩余系，则 $a \cdot x + b$ 也遍历模 m 的一个完全剩余系.

证：根据定理 2.2.2，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 $a \cdot a_0 + b, a \cdot a_1 + b, \cdots, a \cdot a_{m-1} + b$ 模 m 两两不同余.

事实上，若存在 a_i 和 a_j $(i \neq j)$ 使得 $a \cdot a_i + b \equiv a \cdot a_j + b \mod m$，则 $m \mid a \cdot (a_i - a_j)$. 因为 $(a, m) = 1$，我们有 $m \mid a_i - a_j$，这说明 a_i 和 a_j 模 m 同余，与假设矛盾.

因此，$a \cdot x + b$ 也遍历模 m 的一个完全剩余系.

例 2.2.2 设 $m = 12, a = 5, b = 3$，则形如 $a \cdot k + b$ 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 $m_2 \cdot x_1 + m_1 \cdot x_2$ 遍历模 $m_1 \cdot m_2$ 的完全剩余系.

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 $m_2 \cdot x_1 + m_1 \cdot x_2$ 遍历模 $m_1 \cdot m_2$ 的完全剩余系.

证：因为 x_1, x_2 分别遍历 m_1, m_2 个数时，$m_2 \cdot x_1 + m_1 \cdot x_2$ 遍历 $m_1 \cdot m_2$ 个数，所以只需证明这 $m_1 \cdot m_2$ 个整数模 $m_1 \cdot m_2$ 两两不同余.

事实上，若整数 x_1, x_2 和 y_1, y_2 满足

$$m_2 \cdot x_1 + m_1 \cdot x_2 \equiv m_2 \cdot y_1 + m_1 \cdot y_2 \mod (m_1 \cdot m_2),$$

则根据性质 2.1.6，有

$$m_2 \cdot x_1 + m_1 \cdot x_2 \equiv m_2 \cdot y_1 + m_1 \cdot y_2 \mod m_1,$$

即

$$m_2 \cdot x_1 \equiv m_2 \cdot y_1 \mod m_1.$$

进而，$m_1 \mid m_2 \cdot (x_1 - y_1)$. 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，可得 x_2 与 y_2 模 m_2 同余.

因此，结论成立.

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 $m_2\cdot x_1+m_1\cdot x_2$ 遍历模 $m_1\cdot m_2$ 的完全剩余系.

证：因为 x_1,x_2 分别遍历 m_1,m_2 个数时，$m_2\cdot x_1+m_1\cdot x_2$ 遍历 $m_1\cdot m_2$ 个数，所以只需证明这 $m_1\cdot m_2$ 个整数模 $m_1\cdot m_2$ 两两不同余.

事实上，若整数 x_1,x_2 和 y_1,y_2 满足

$$m_2\cdot x_1+m_1\cdot x_2\equiv m_2\cdot y_1+m_1\cdot y_2 \mod (m_1\cdot m_2),$$

则根据性质 2.1.6，有

$$m_2\cdot x_1+m_1\cdot x_2\equiv m_2\cdot y_1+m_1\cdot y_2 \mod m_1,$$

即
$$m_2\cdot x_1\equiv m_2\cdot y_1 \mod m_1.$$

进而，$m_1\mid m_2\cdot(x_1-y_1)$. 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，可得 x_2 与 y_2 模 m_2 同余.

因此，结论成立. —— (为什么？)

例 2.2.3 设 p,q 是两个不同的素数, n 是它们的乘积, 则对于任意的整数 c, 存在唯一的一对整数 x,y 满足

$$q\cdot x+p\cdot y\equiv c \mod n,\ 0\leqslant x<p, 0\leqslant y<q.$$

例 2.2.3 设 p,q 是两个不同的素数, n 是它们的乘积, 则对于任意的整数 c, 存在唯一的一对整数 x,y 满足

$$q\cdot x+p\cdot y\equiv c \mod n,\ 0\leqslant x<p, 0\leqslant y<q.$$

证：因为 p,q 是两个不同的素数, 所以 p,q 互素.

根据定理 2.2.4 及其证明知,

当 x,y 分别遍历模 p,q 的完全剩余系时, $q\cdot x+p\cdot y$ 遍历模 $n=p\cdot q$ 的完全剩余系.

因此, 对于任意的整数 c, 存在唯一的一对整数 x,y 满足

$$q\cdot x+p\cdot y\equiv c \mod n,\ 0\leqslant x<p, 0\leqslant y<q.$$

本课作业

1. 证明: 设 a 与 b 是整数, k 与 m 是正整数, 且 $a \equiv b \mod m$, 则 $a^k \equiv b^k \mod m$.

2. 求十进制数 777^{777} 的个位是几?

3. 证明: 形如 $8k+7$ 的正整数都不能表示为三个平方数之和.

4. 写出模 9 的两个完全剩余系. 要求: 其中一个完全剩余系中每个数均为奇数, 另一个中每个数均为偶数. 此外, 问对模 10 能否写出这样的两个完全剩余系?

交流与讨论

电子邮箱：

陈秀波：xb_chen@bupt.edu.cn

徐国胜：guoshengxu@bupt.edu.cn

金正平：zhpjin@bupt.edu.cn