信息安全的数学基础 (1)

唐　灯

上海交通大学网络空间安全学院

第一章 预备知识

§1.1 数论预备知识

§1.2 集合论预备知识

§1.1 数论预备知识

- 整除
- 整除的性质
- 辗转相除法 (更相减损术)
- 算数基本定理
- 同余
- 同余的性质
- 中国剩余定理
- RSA 和 Rabin 公钥密码方案

整除

定义 1

设 $a, b \in \mathbb{Z}$, 其中 $b \neq 0$, 如果存在一个整数 q 使得等式

$$a = qb$$

成立, 我们就说 b **整除** a 或 a 被 b 整除, 记作 $b \mid a$, 此时我们把 b 叫作 a 的**因子**, 把 a 叫作 b 的**倍数**. 如果整数 q 不存在, 我们就说 b 不能整除 a 或 a 不被 b 整除, 记作 $b \nmid a$.

注 1.1

对任意 $a, b, c \in \mathbb{Z}$, 由整除的定义可得:

(1) $b \mid a$, 则 $b \mid ta$, 其中 $t \in \mathbb{Z}$;
(2) $b \mid a$ 且 $a \mid b$, 则 $a = \pm b$;
(3) a, b 都是 m 的倍数, 则 $sa \pm tb$ 也是 m 的倍数, 其中 $s, t \in \mathbb{Z}$;
(4) $c \mid b$ 且 $b \mid a$, 则 $c \mid a$.

素数

定义 2

如果整数 $p > 1$, 并且 p 只能被 ± 1 和 $\pm p$ 整除, 那么称 p 为**素数** (prime number).

定理 3 (带余除法)

若 $a, b \in \mathbb{Z}$, 其中 $b > 0$, 则存在 $q, r \in \mathbb{Z}$, 使得

$$a = qb + r, 0 \leq r < b$$

成立, 而且 q 及 r 是惟一的. 其中 q 叫做 a 被 b 除所得的**不完全商**, r 叫作 a 被 b 除所得到的**余数**.

证明

作整数序列

$$\cdots, -3b, -2b, -b, 0, b, 2b, 3b, \cdots$$

则 a 必在上述序列的某两项之间, 即存在一个整数 q 使得

$$qb \leq a < (q+1)b$$

成立. 令 $a - qb = r$, 则 $a = qb + r$ 且 $0 \leq r < b$. 下面我们用反证法证明 q, r 的惟一性. 设 $q_1, r_1 \in \mathbb{Z}$ 且 $a = q_1 b + r_1, 0 \leq r_1 < b$, 则有

$$q_1 b + r_1 = qb + r,$$

于是

$$(q - q_1)\, b = r_1 - r,$$

可得

$$|q - q_1| b = |r_1 - r|.$$

由于 r 及 r_1 都是小于 b 的非负数, 所以上式右边是小于 b 的. 如果 $q \neq q_1$ 则上式左边大于 b. 这是不可能的. 因此 $q = q_1$ 从而 $r = r_1$.

最大公因子

定义 4

设 $a_1, a_2, \cdots, a_n$ 是 n $(n \geq 2)$ 个整数. 若整数 d 是它们之中每一个的因子, 那么 d 就叫作 $a_1, a_2, \cdots, a_n$ 的**一个公因子**. 整数 $a_1, a_2, \cdots, a_n$ 的公因子中最大的一个叫作**最大公因子** (greatest common divisor), 记作 $(a_1, a_2, \cdots, a_n)$ 或 $\gcd(a_1, a_2, \cdots, a_n)$. 特别地, 若 $(a_1, a_2, \cdots, a_n) = 1$, 我们称 $a_1, a_2, \cdots, a_n$ **互素**; 若 $a_1, a_2, \cdots, a_n$ 中任意两个不同的整数都互素, 我们就称它们**两两互素**.

最大公因子的性质

注 4.1

(1) 任意非零 $a, b \in \mathbb{Z}$ 的最大公因子为正整数, 且 $(a, b) = (|a|, |b|)$;

(2) 0 可被任意非零整数整除, 故对任意非零整数 b 有 $(0, b) = |b|$.

证明: (1) 设 d 是 a, b 的任一公因子, 由定义 $d \mid a$ 且 $d \mid b$, 因而 $d \mid |a|$ 且 $d \mid |b|$, 故 d 是 $|a|, |b|$ 的一个公因子, 同法可证, $|a|, |b|$ 的任一公因子都是 a, b 的一个公因子, 所以 a, b 和 $|a|, |b|$ 有相同的公因子, 也即具有相同的最大公因子.

(2) 由于任何非零整数都是 0 的因子, 故 $|b|$ 的每一个因子均是 0 与$|b|$ 的公因子. 由于 $|b|$ 的最大正因子是 $|b|$,
故$(0, b) = (0, |b|) = |b|$.

最大公因子的性质

定理 5

设 a, b 是两个不全为零的整数, 令 $S = \{xa + yb > 0 \mid x, y \in \mathbb{Z}\}$, 则 $(a, b) = \min S$.

证明: 不失一般性, 假定 $b \neq 0$. 首先证明 $S \neq \emptyset$. 若 $b > 0$, 则 $b = 0a + 1b \in S$, 若 $b < 0$ 则 $-b = 0a + (-1)b \in S$. 设 $d = \min S = ma + nb > 0$, 其中 $m, n \in \mathbb{Z}$. 以下证明 $d = (a, b)$. 注意到 a 可写为 $a = qd + r$, 其中 $0 \leq r < d$. 于是,

$$r = a - qd = a - q(ma + nb) = (1 - qm)a + (-qn)b.$$

若 $r > 0$, 则有 $r \in S$. 注意到 $r < d$, 这与 d 的定义矛盾, 故 $r = 0$. 于是 $a = dq$, 由此 $d \mid a$. 类似地, 考虑 $b = q'd + r'$, 其中 $0 \leq r' < d$, 可得 $r' = 0$, 从而 $d \mid b$. 因此 d 是 a 与 b 的公因子. 由于 (a, b) 为最大公因子, 故 $d \leq (a, b)$. 另一方面, 由于 $(a, b) \mid a$ 且 $(a, b) \mid b$, 由注 1.1 第 (3) 条可得 $(a, b) \mid d$, 从而 $(a, b) \mid d$, 于是 $(a, b) \leq d$. 因此可得 $d = (a, b)$.

最大公因子的性质

定理 6

设 a, b 是两个正整数, 则存在整数 m, n 使得 $(a, b) = ma + nb$.

注 6.1

定理 *6* 中的整数 m, n 不唯一. 事实上有:

$$\begin{aligned}(a, b) &= ma + nb \\ &= ma - ab + nb + ab \\ &= (m - b)a + (n + a)b = m'a + n'b.\end{aligned}$$

最大公因子的性质

推论 7

设 a, b 是两个都不为零的整数, 则 a 与 b 的公因子都是 (a, b) 的因子.

定理 8

设 a, b 是两个都不为零的整数, 如果正整数 d 满足下述两个条件:

(1) $d \mid a$ 且 $d \mid b$;
(2) 若 $c \mid a$ 且 $c \mid b$, 则 $c \mid d$,

则 d 是 a 与 b 的最大公因子.

证明: 令 $(a, b) = d' > 0$. 由定理 6 可知存在 $m, n \in \mathbb{Z}$ 使得 $d' = ma + nb$. 由 (1) 和注 1.1 第 (3) 条立即可得 $d \mid d'$. 在 (2) 中取 $c = d'$ 立即可得 $d' \mid d$. 综上可得 $d = d'$.

最大公因子的性质

定理 9

如果 a 和 b 是不全为零的两个整数, 则 $(a,b)=1$ 当且仅当存在整数 m,n 使得 $ma+nb=1$.

证明: 若 $(a,b)=1$, 则由定理 6 知存在整数 m,n 使得 $ma+nb=1$. 相反地, 若有 $ma+nb=1$. 如果 $d=(a,b)>0$ 则 $d \mid a$ 且 $d \mid b$, 于是由注 1.1 第 (3) 条可得 $d \mid ma+nb$. 从而有 $d \mid 1$, 于是 $d=1$.

最大公因子的性质

定理 10

若 a, b, c 是三个整数, 且 $(a, c) = 1$, 则:

(1) ab, c 与 b, c 有相同的公因子;

(2) 若 b, c 不全为零则 $(ab, c) = (b, c)$.

证明: (1) 由 $(a, c) = 1$ 知存在两个整数 m, n 使得 $ma + nc = 1$. 两边乘以 b 得 $mab + ncb = b$. 设 d 是 ab 和 c 的任一公因子, 则 $d \mid b$, 因而 d 是 b, c 的一个公因子. 反之 b, c 的任一公因子显然是 ab, c 的一个公因子. 于是 (1) 得证.

(2) 因为 b, c 不全为零, 故 (b, c) 是存在的, 因而由 (1) 即知 (ab, c) 存在且 $(ab, c) = (b, c)$.

最大公因子的性质

推论 11

若 a, b, c 是三个整数, 则:

(1) 若 $(a, c) = 1$ 且 $(b, c) = 1$, 则 $(ab, c) = 1$;
(2) 若 $(a, c) = 1$ 且 $c \mid ab$, 则 $c \mid b$;
(3) 若 c 为素数且 $c \mid ab$, 则 $c \mid a$ 或 $c \mid b$.

证明: (1) 若 $(a, c) = 1$, 则由定理 10 第 (2) 立即可得 $(ab, c) = (b, c) = 1$.

(2) $b = 0$ 时显然成立. 当 $b \neq 0$ 时由定理 10 第 (2) 条可设 $(ab, c) = (b, c) = d$. 若有 $c \mid ab$, 则 c 为 ab 和 c 的公因子, 由推论 7 可知 $c \mid d$. 又 $d \mid b$, 故 $c \mid b$.

(3) 因为 c 为素数, 若$c \nmid a$ 则 $(a, c) = 1$, 由 (1) 得 $c \mid b$.

定理 12

设 a, b, c 是任意三个不全为 0 的整数, 且有 $a = qb + c$, 其中 $q \neq 0$. 则 a, b 与 b, c 有相同的公因子, 因而 $(a, b) = (b, c)$.

证明: 设 d 是 a, b 的任一公因子, 由定义知 $d \mid a, d \mid b$. 于是 d 是 $c = a + (-q)b$ 的因子, 因而 d 是 b, c 的一个公因子. 同法可证 b, c 的任一公因子是 a, b 的一个公因子. 于是定理的前一部分获证, 第二部分显然随之成立.

注 12.1

由定理 *12* 可得对任意 $a, m \in \mathbb{Z}$ 有 $(a, m) = (a + tm, m)$, 其中 $t \in \mathbb{Z}$.

- 由此可知 $(a_1, a_2, \cdots, a_n) = (|a_1|, |a_2|, \cdots, |a_n|)$. 给定两个正整数 a, b, 由带余除法有下列等式:

$$\begin{aligned}
a &= q_1 b + r_1,\ 0 \le r_1 < b \\
b &= q_2 r_1 + r_2,\ 0 \le r_2 < r_1 \\
r_1 &= q_3 r_2 + r_3,\ 0 \le r_3 < r_2 \\
r_2 &= q_4 r_3 + r_4,\ 0 \le r_4 < r_3 \\
&\cdots \quad \cdots \quad \cdots \\
r_{n-2} &= q_n r_{n-1} + r_n,\ 0 \le r_n < r_{n-1}, \\
r_{n-1} &= q_{n+1} r_n + r_{n+1},\ r_{n+1} = 0.
\end{aligned} \tag{1}$$

辗转相除法

- 因为每进行一次带余数除法, 余数就至少减一, 而 b 是有限的, 所以我们最多进行 b 次带余数除法就可以得到一个余数是零的等式.
- 反复运用定理 12, 可以计算出两个正整数的最大公因子, 该方法称为**辗转相除法** (在西方常把它叫做欧几里得除法), 它也是我国著名的古代数学著作《九章算术》中提出的 "更相减损术".
- 例如, 可由下列步骤求 $(169, 121)$:

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

于是有 $(169, 121) = 1$. 进一步, 注意到 $1 = 23 - 11 \times 2 = 23 - 11(25 - 1 \times 23) = \cdots = 58 \times 169 - 81 \times 121$.

最小公倍数

定义 13

设 $a_1, a_2, \cdots, a_n$ 是 n $(n \geqslant 2)$ 个整数. 若 d 是这 n 个数的倍数, 则 d 就叫作这 n 个数的**一个公倍数**. 又在 $a_1, a_2, \cdots, a_n$ 的一切公倍数中的最小正数叫作**最小公倍数** (least common multiple), 记作 $[a_1, a_2, \cdots, a_n]$ 或 $\operatorname{lcm}(a_1, a_2, \cdots, a_n)$.

注 13.1

由于任何正数都不是 0 的倍数, 故讨论整数的最小公倍数时, 一概假定这些整数都不是零.

最小公倍数的性质

定理 14

设 a, b 是任意两个正整数, 则:

(1) a, b 的所有公倍数就是 $[a, b]$ 的所有倍数;

(2) $[a, b] = \frac{ab}{(a,b)}$.

算数基本定理

定理 15 (算术基本定理)

设 a 是任一大于 1 的整数, 则 a 可表为素数的乘积, 即

$$a = p_1 p_2 \cdots p_n,\ p_1 \le p_2 \le \cdots \le p_n,$$

其中 $p_1, p_2, \cdots, p_n$ 是素数. 并且若

$$a = q_1 q_2 \cdots q_m,\ q_1 \le q_2 \le \cdots \le q_m,$$

其中 $q_1, q_2, \cdots, q_m$ 是素数, 则 $m = n, q_i = p_i, i = 1, 2, \cdots, n.$

证明: 我们首先用归纳法证明 a 可表为素数的乘积. 显然 $a = 2$ 时成立. 假定对一切小于 a 的正整数均成立. 现在讨论 a. 若 a 是素数, 显然成立; 若 a 是合数, 则有两正整数 b, c 满足条件

$$a = bc, 1 < b < a, 1 < c < a.$$

由假定

$$b = p_1' p_2' \cdots p_l',\ c = p_{l+1}' p_{l+2}' \cdots p_n',$$

于是

$$a = p_1' p_2' \cdots p_l' p_{l+1}' \cdots p_n'.$$

证明 (续)

将 p_i' 的顺序适当调动后即满足定理描述的第一部分, 由数学归纳法可得 (1) 对于任意大于 1 的正整数成立.

现证明 $n = m, p_k = q_k, k = 1, 2, \cdots, n$. 若有 $a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m$. 此时有 $p_1 \mid q_1 q_2 \cdots q_m$. 则一定有 $q_j, j \in \{1, \cdots, m\}$ 使得 $p_1 \mid q_j$, 因为 p_1, q_j 是素数, 则 $p_1 = q_j$, 对 q_1 同理, 即一定有 $i \in \{1, \cdots, m\}$ 满足 $p_i = q_1$. 又 $p_i \geq p_1, q_j \geq q_1$, 故 $q_j = p_1 \leq p_i = q_1$, 于是 $q_1 \geq q_j$. 又 $q_1 \leq q_j$, 故 $q_j = q_1$, 进而 $p_1 = q_1$. 以此类推即得 $n = m, p_k = q_k, k = 1, 2, \cdots, n$.

推论 16

设 a 是任一大于 1 的整数, 则 a 能够惟一地写成

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \alpha_i > 0, i = 1, \cdots, k,$$

其中 p_i $(1 \leq i \leq k)$ 为素数且对任意 $1 \leq i < j \leq k$ 都有$p_i < p_j$. 该式称作 a 的标准分解式. 并且 a 的正因子 d 可表示成如下形式:

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \alpha_i \geq \beta_i \geq 0, i = 1, 2, \cdots, k.$$

证明: 将定理 15 的分解式进行整理立即可得 a 的唯一性表示.

若 $d \mid a$, 则 $a = dq$, 由于 a 的标准分解式是惟一的, 故 d 的标准分解式中出现的素数都在 p_j $(j = 1, 2, \cdots, k)$ 中出现, 且 p_j 在 d 的标准分解式中出现的指数 $\beta_j \not> \alpha_j$, 亦即 $\beta_j \leq \alpha_j$. 反过来当 $\beta_j \leq \alpha_j$ 时, d 显然整除 a.

同余

定义 17

给定一个正整数 m, 如果用 m 去除任意两个整数 a 与 b 所得的余数相同, 我们就说 a, b 对模 m **同余**, 记作 $a \equiv b \pmod{m}$. 如果余数不同, 我们就说 a, b 对模 m **不同余**, 记作 $a \not\equiv b \pmod{m}$.

注 17.1

设 m 是任一正整数, 则模 m 的同余是等价关系, 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 $a \equiv c \pmod{m}$.

同余

定理 18

整数 a, b 对模 m 同余的充分与必要条件是 $m \mid a-b$, 即 $a = b + tm$, 其中 $t \in \mathbb{Z}$.

证明: 设 $a = q_1 m + r_1, b = q_2 m + r_2, 0 \leq r_1 < m, 0 \leq r_2 < m$.

若 $a \equiv b \pmod{m}$, 则 $r_1 = r_2$, 于是 $a - b = (q_1 - q_2)m$, 因此 $m \mid a - b$, 即 $a = b + tm$, 其中 $t = q_1 - q_2$.

反之, 若 $m \mid a - b$, 则 $m \mid (q_1 - q_2)m + (r_1 - r_2)$, 即存在 $q \in \mathbb{Z}$ 使得 $(q_1 - q_2)m + (r_1 - r_2) = qm$, 于是 $r_1 - r_2 = (q - q_1 + q_2)m$, 因此 $m \mid r_1 - r_2$. 但 $|r_1 - r_2| < m$, 故 $r_1 = r_2$.

注 18.1

定理 *18* 说明同余这一概念又可定义为: 若 $m \mid a - b$, 则 a, b 叫做对模 m 同余.

同余的性质

定理 19

若 $a \equiv b \pmod{m}, u \equiv v \pmod{m}$, 则:

(1) $ax + uy \equiv bx + vy \pmod{m}$, 其中 $x, y \in \mathbb{Z}$;
(2) $au \equiv bv \pmod{m}$;
(3) $f(a) \equiv f(b) \pmod{m}$, 其中 $f(x)$ 为任意给定的一个整系数多项式.

证明: (1) 由定理 18 有 $m \mid a - b$ 且 $m \mid u - v$. 于是

$$m \mid (a-b)x + (u-v)y \Rightarrow m \mid (ax + uy) - (bx + vy).$$

由定理 18 即知 $ax + uy \equiv bx + vy \pmod{m}$.

(2) 由定理 18 有 $m \mid a - b$ 且 $m \mid u - v$. 于是
$m \mid (a-b)u + b(u-v)$, 即 $m \mid au - bv$, 从而 $au \equiv bv \pmod{m}$.

(3) 由 (1)和 (2) 立即可得.

同余的性质

定理 20

若 $a \equiv b \pmod{m}$, 则下述三条成立:

(1) $a_1 \equiv b_1 \pmod{m}$, 其中 $a = a_1 d, b = b_1 d, (d, m) = 1$;
(2) $a \equiv b \pmod{d}$, 其中 $d \mid m$ 且 $d > 0$;
(3) $(a, m) = (b, m)$, 因而若 d 能整除 m 及 a, b 二数之一, 则 d 必能整除 a, b 中的另一个.

证明: (1) 由定理 18 得 $m \mid a - b$. 由于 $a - b = d(a_1 - b_1)$, 故 $m \mid d(a_1 - b_1)$. 因为 $(d, m) = 1$, 由推论 11 中 (2) 可知 $m \mid a_1 - b_1$, 于是 $a_1 \equiv b_1 \pmod{m}$.

(2) 由定理 18 得 $m \mid a - b$, 因为 $d \mid m, d > 0$, 由整除的传递性 (注 1.1 中 (4)) 可知 $d \mid a - b$, 再次由定理 18 可得 $a \equiv b \pmod{d}$.

(3) 由定理 18 知存在 t 使得 $a = tm + b$. 由定理 12 立即可得 $(a, m) = (b, m)$. 进一步, 易得若 d 能整除 m 及 a, b 二数之一, 则 d 必能整除 a, b 中的另一个.

同余的性质

定理 21

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

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

剩余类

定义 22

若 m 是一个给定的正整数, 则全部整数可分成 m 个集合, 记作 $C_0, C_1, \cdots, C_{m-1}$, 其中 $C_r\ (r = 0, 1, \cdots, m-1)$ 表示所有形如 $qm + r\ (q = 0, \pm 1, \pm 2, \cdots)$ 的整数组成的集合, 则 $C_0, C_1, \cdots, C_{m-1}$ 叫做模 m 的**一个剩余类**.

注 22.1

设 m 是任一正整数, $C_0, C_1, \cdots, C_{m-1}$ 是模 m 的一个剩余类, 则:

(1) 若有 $(r, m) = 1$, 则由定理 *12* 或注 *12.1* 知 C_r 中所有的数均与 m 互素;

(2) 在数论中, 通常将 C_r 记做 $\bar{r}$, 并将 $C_0, C_1, \cdots, C_{m-1}$ 构成的集合称为剩余类集, 记为 $\mathbb{Z}_m$, 即 $\mathbb{Z}_m = \{\bar{0}, \bar{1}, \cdots, \overline{m-1}\}$.

剩余类的性质

定理 23

若 m 是一个给定的正整数, 则 $C_0, C_1, \cdots, C_{m-1}$ 具有下列性质:

(1) 对任一 $a \in \mathbb{Z}$, 则存在唯一的 $0 \leq r \leq m-1$ 使得 $a \in C_r$;

(2) 对任一 $0 \leq r \leq m-1$ 以及 $a, b \in \mathbb{Z}$, 则 $a, b \in C_r$ 当且仅当 $a \equiv b \equiv r \pmod{m}$.

证明: (1) 由定理 3 知存在唯一整数 q 和 $0 \leq r < m$ 使得

$$a = qm + r,$$

故 a 在 C_r 内且 r 由 a 惟一确定.

(2) 由题设有

$$a = q_1 m + r, b = q_2 m + r,$$

故 $a \equiv b \pmod{m}$. 反之若 $a \equiv b \equiv r \pmod{m}$, 则由同余的定义即知 $a, b \in C_r$.

完全剩余系

定义 24 (完全剩余系)

设 m 是一个给定的正整数, 若 $a_0, a_1, \cdots, a_{m-1}$ 是 m 个整数, 并且其中任何两数都不同在一个剩余类里, 则 $a_0, \cdots, a_{m-1}$ 叫做模 m 的一个**完全剩余系**.

定理 25

m 个整数组成模 m 的一个完全剩余系的充分与必要条件是两两对模 m 不同余.

定理 26

设 m 是正整数, $(a, m) = 1$, b 是任意整数, 若 $a_0, a_1, \cdots, a_{m-1}$ 是模 m 的一个完全剩余系, 则 $aa_0 + b$, $aa_1 + b, \cdots, aa_{m-1} + b$ 也是模 m 的一个完全剩余系.

证明: 由定理 25, 我们只需证明 $aa_0 + b, aa_1 + b, \cdots, aa_{m-1} + b$ 两两不同余即可. 我们用反证法来证明. 假定有 $aa_i + b \equiv aa_j + b \pmod{m}$, $i \neq j$. 则由定理 19 第 (1) 条可得 $aa_i \equiv aa_j \pmod{m}$. 又因为 $(a, m) = 1$, 由定理 20 第 (1) 条可得 $a_i \equiv a_j \pmod{m}$, 这与 $a_0, a_1, \cdots, a_{m-1}$ 是模 m 的一个完全剩余系矛盾. 从而 $aa_0 + b$, $aa_1 + b, \cdots, aa_{m-1} + b$ 中没有两个数对模 m 同余, 由定理 25 即得它们是模 m 的一个完全剩余系.

例

例 27

由定理 26 我们知道下述序列都是模 m 的完全剩余系:

$$0, 1, \cdots, m-1;$$

$$-m, 1-m, \cdots, a-m, \cdots, -1;$$

$$0, m+1, \cdots, a(m+1), \cdots, (m-1)(m+1).$$

完全剩余系

定理 28

设 m, n 是两个互素的正整数. $x_1, x_2, \cdots, x_m$ 是模 m 的一个完全剩余系, $y_1, y_2, \cdots, y_n$ 是模 n 的一个完全剩余系, 则 $my_1 + nx_1, my_1 + nx_2, \cdots, my_1 + nx_m, \cdots, my_n + nx_1, my_n + nx_2, \cdots, my_n + nx_m$ 是模 mn 的一个完全剩余系.

证明: 只需证明这 mn 个整数对模 mn 两两不同余即可. 假定

$$my_i + nx_j \equiv my_{i'} + nx_{j'} \pmod{mn},$$

其中 $x_j, x_{j'}$ 取自 $x_1, x_2, \cdots, x_m$, $y_i, y_{i'}$ 取自 $y_1, y_2, \cdots, y_n$. 注意到 m, n 都整除 mn. 因此, 由定理 20 第 (2) 条得

$$my_i + nx_j \equiv my_{i'} + nx_{j'} \pmod{m},$$

$$my_i + nx_j \equiv my_{i'} + nx_{j'} \pmod{n}.$$

证明 (续)

于是

$$nx_j \equiv nx_{j'} \pmod{m},$$

$$my_i \equiv my_{i'} \pmod{n}.$$

注意到 $(m,n)=1$, 由定理 20 第 (1) 条即得 $x_j \equiv x_{j'} \pmod{m}$, $y_i \equiv y_{i'} \pmod{n}$. 于是 $x_j = x_{j'}$, $y_i = y_{i'}$. 因此定理获证.

简化剩余系

定义 29 (简化剩余系)

如果一个模 m 的剩余类里面的数与 m 互素, 就把它叫做一个**与模 m 互素的剩余类**. 在与模 m 互素的全部剩余类中, 从每一类中任取一数所作成的集合叫做模 m 的一个**简化剩余系** (也称既约剩余系或缩系).

注 29.1

由定理 *3* 知模 m 的剩余类与模 m 互素的充分与必要条件是此类中有一数与 m 互素, 即 C_r 为与模 m 互素的剩余类当且仅当 $(r, m) = 1$.

欧拉函数

定义 30 (欧拉 (Euler) 函数)

欧拉函数 $\varphi(n)$ 是定义在正整数上的函数, 它在正整数 n 上的值等于序列 $1, 2, \cdots, n-1$ 中与 n 互素的数的个数.

注 30.1

由欧拉函数可知:

(1) 若 n 是素数, 则 $\varphi(n) = n - 1$;
(2) 模 m 的每个简化剩余系含有 $\varphi(m)$ 个元素.
(3) 模 m 的每个简化剩余系是由与 m 互素的 $\varphi(m)$ 个对模 m 不同余的整数组成的.

简化剩余系

定理 31

设 $x_1, x_2, \cdots, x_{\varphi(m)}$ 是模 m 的一个简化剩余系. 若 $(a, m) = 1$, 则 $ax_1, ax_2, \cdots, ax_{\varphi(m)}$ 是模 m 的一个简化剩余系.

证明: 由于 $(a, m) = 1$ 且对任意 $1 \leq i \leq \varphi(m)$ 有 $(x_i, m) = 1$, 故 $(ax_i, m) = 1$. 并且, 对任意 $1 \leq i \neq j \leq \varphi(m)$, 若 $ax_i \equiv ax_j \pmod{m}$, 则有 $x_i \equiv x_j \pmod{m}$. 故 $ax_1, ax_2, \cdots, ax_{\varphi(m)}$ 是 $\varphi(m)$ 个与 m 互素的整数, 且两两不同余, 是模 m 的一个简化剩余系.

Euler 定理

定理 32 (Euler 定理)

设 n 是大于 1 的整数. 若 $(a,n)=1$, 则 $a^{\varphi(n)} \equiv 1 \pmod{n}$.

证明: 设 $x_1, x_2, \cdots, x_{\varphi(n)}$ 是模 n 的一个简化剩余系, 由定理 31 知

$$ax_1, ax_2, \cdots, ax_{\varphi(n)}$$

也是模 n 的一个简化剩余系. 由定理 19 第 (2) 条得

$$(ax_1)(ax_2)\cdots(ax_{\varphi(n)}) \equiv x_1x_2\cdots x_{\varphi(n)} \pmod{n},$$

即

$$a^{\varphi(n)}x_1x_2\cdots x_{\varphi(n)} \equiv x_1x_2\cdots x_{\varphi(n)} \pmod{n}.$$

又因为 $(x_1,n)=(x_2,n)=\cdots=(x_{\varphi(n)},n)=1$, 由推论 11 第 (1) 条可得 $(x_1x_2\cdots x_{\varphi(n)},n)=1$. 于是, 由定理 20 第 (1) 条即得

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

Fermat 小定理

推论 33 (Fermat 小定理)

若 p 是素数, 则 $a^p \equiv a \pmod{p}$.

证明: 若$(a,p)=1$, 则由定理 32 可得 $a^{\varphi(p)} \equiv 1 \pmod{p}$. 注意到 $\varphi(p)=p-1$, 可得 $a^{p-1} \equiv 1 \pmod{p}$. 由定理 19 第 (2) 条立即可得 $a^p \equiv a \pmod{p}$. 若$(a,p)\neq 1$, 则 $p \mid a$, 于是 $p \mid a^p - a$. 由定理 18 即得 $a^p \equiv a \pmod{p}$.

简化剩余系

定理 34

设 m, n 是两个互素的正整数. $x_1, x_2, \cdots, x_{\varphi(m)}$ 是模 m 的一个简化剩余系, $y_1, y_2, \cdots, y_{\varphi(n)}$ 是模 n 的一个简化剩余系, 则 $my_1 + nx_1, my_1 + nx_2, \cdots, my_1 + nx_{\varphi(m)}, \cdots, my_{\varphi(n)} + nx_1, my_{\varphi(n)} + nx_2, \cdots, my_{\varphi(n)} + nx_{\varphi(m)}$ 是模 mn 的一个简化剩余系.

欧拉定理的性质

推论 35

若 m, n 是两个互素的正整数, 则 $\varphi(mn) = \varphi(m)\varphi(n)$. 特别地, 若 m, n 是两个不相同的素数, 则 $\varphi(mn) = (m-1)(n-1)$.

证明: 由注 22.1 第 (1) 以及简化剩余系的定义可知 $\varphi(mn)$ 等于模 mn 的简化剩余系中元素的个数, 由定理 34 立即可得 $\varphi(mn) = \varphi(m)\varphi(n)$. 特别地, 若 m, n 是素数, 则 $\varphi(m) = m-1, \varphi(n) = n-1$.

欧拉定理的性质

定理 36

若 $n = p^t$, 其中 p 是素数, 则 $\varphi(n) = p^t - p^{t-1}$.

证明: 显然, p^t 的因子都是 p 的幂次. 因此任何小于等于 n 且是 p 的倍数的数都与 p 有大于 1 的最大公因子, 而其它小于等于 n 的非负整数都与 p 互素. 注意到小于 n 的正整数中 p 的倍数有 $p, 2p, \cdots, (p^{t-1} - 1) \cdot p$, 其个数为 $p^{t-1} - 1$. 于是可得 $\varphi(p^t) = (p^t - 1) - (p^{t-1} - 1) = p^t - p^{t-1}$.

欧拉定理的性质

定理 37

设 $n = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$, 其中 $p_1, p_2, \cdots, p_s$ 是 s 个两两不同的素数. 则

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_s}\right).$$

证明: 由推论 35 易得

$$\varphi(n) = \varphi(p_1^{t_1})\varphi(p_1^{t_2})\cdots\varphi(p_1^{t_s}).$$

由定理 36 知, 当 p 是素数时

$$\varphi(p^t) = p^t - p^{t-1}.$$

综上即得

$$\begin{aligned}\varphi(n) &= (p_1^{t_1} - p_1^{t_1-1})(p_2^{t_2} - p_2^{t_2-1})\cdots(p_s^{t_s} - p_s^{t_s-1}) \\ &= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_s}\right).\end{aligned}$$

同余式

定义 38 (同余式)

若用 $f(x)$ 表示多项式 $a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$, 其中 $n > 0$, a_i $(i = 1, 2, \cdots, n)$ 是整数. 又设 m 是一个正整数, 则

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

叫做模 m 的同余式. 若 $a_n \not\equiv 0 \pmod{m}$, 则 n 叫做同余式的次数. 若 a 是使 $f(a) \equiv 0 \pmod{m}$ 成立的一个整数, 则 $x \equiv a \pmod{m}$ 叫做同余式的一个解, 并且把满足 $f(x) \equiv 0 \pmod{m}$ 且对 m 相互同余的一切数算作同余式的一个解.

一次同余式

主要关注一次同余式:

$$x \equiv b_1 \pmod{m_1},\ x \equiv b_2 \pmod{m_2}, \cdots, x \equiv b_k \pmod{m_k}.$$

例 39

在我国古代的《孙子算经》里提出了一个问题: “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? ” 设 x 是所求物数, 则依题意可得一次同余式组:

$$x \equiv 2 \pmod{3},\ x \equiv 3 \pmod{5},\ x \equiv 2 \pmod{7}.$$

引理 40

设 p 是素数, a 是任一整数. 若有 $(a,p)=1$, 则存在唯一整数 $0 \leq m < p$ 使得 $ma \equiv 1 \pmod{p}$.

证明: 由定理 6 知存在整数 m,n 使得 $ma+np=1$, 于是对任意整数 t 都有 $(m-tp)a+(n+ta)p=1$, 因此必有 m_1,n_1 使得 $m_1a+n_1p=1$ 且 $0 \leq m_1 < p$. 下证 m_1 的唯一性. 假设存在 m_2,n_2 使得 $m_2a+n_2p=1$ 且 $0 \leq m_2 < p$, 则有 $(m_1-m_2)a=(n_1-n_2)p$, 于是 $p \mid (m_1-m_2)a$. 由推论 11 第 (3) 条以及 $(a,p)=1$ 立即可得 $p \mid m_1-m_2$. 由于 $|m_1-m_2| < p$, 故 $m_1-m_2=0$, 即 $m_2=m_1$.

中国剩余定理

定理 41 (中国剩余定理)

设 $m_1, m_2, \cdots, m_k$ 是 k 个两两互素的正整数，
$m = m_1 m_2 \cdots m_k$, $M_i = m/m_i, i = 1, 2, \cdots, k$, 则同余式组
$x \equiv b_1 \pmod{m_1}$, $x \equiv b_2 \pmod{m_2}$, $\cdots$, $x \equiv b_k \pmod{m_k}$
的解是

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

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

证明: 注意到对任意 $i \neq j$ 有 $(m_i, m_j) = 1$, 于是由推论 11 第 (1) 条可得 $(M_i, m_i) = 1$, 故对每一个 M_i, 由引理 40 知存在 M_i' 使得

$$M_i' M_i \equiv 1 \pmod{m_i}.$$

证明 (续)

另一方面, 由于 $m = m_i M_i$, 因此 $m_j \mid M_i, i \neq j$, 于是

$$\sum_{j=1}^{k} M_j' M_j b_j \equiv M_i' M_i b_i \equiv b_i \pmod{m_i}$$

即为定理中同余式组的解.

下证解的唯一性. 若 x_1, x_2 是定理中同余式组的任意两个整数解, 则

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

因 $(m_i, m_j) = 1$, 于是由定理 21 可得 $x_1 \equiv x_2 \pmod{m}$, 故同余式组的解具有唯一性.

RSA 公钥密码方案

(1) **密钥的产生**:
随机选两个不同的大素数 p 和 q, 计算 $n = pq$, $\varphi(n) = (p-1)(q-1)$; 任意选取一个大整数 $1 \leq e \leq \varphi(n)$ 满足 $(\varphi(n), e) = 1$; 计算d, 满足 $de \equiv 1 \pmod{\varphi(n)}$. 以 $\{e, n\}$ 为公钥, $\{d, n\}$ 为私钥.

(2) **加密运算**:
对明文 $m < n$ 进行加密:

$$c = E(m) \equiv m^e \pmod{n}.$$

(3) **解密运算**:
接收方对 c 进行解密:

$$m = D(c) \equiv c^d \pmod{n}.$$

Rabin 公钥密码方案

Rabin 公钥密码方案

随机选取两个大素数 p, q, 并且 $p \equiv q \equiv 3 \pmod 4$, 令 $n = pq$. 以 $\{n\}$ 为公钥, $\{p, q\}$ 为私钥. 将明文 m 加密为 $c \equiv m^2 \pmod n$.

§1.2 集合论预备知识

- 集合的定义
- 集合的基本运算
- 集合的映射
- 等价关系
- 集合的分类

集合的定义

定义 42

将一些不同的对象放在一起, 即为**集合** (set), 其中的对象称为集合的元素 (element). 通常使用大写字母 $A, B, C, \cdots$ 来表示集合, 用小写字母 $a, b, c, \cdots$ 来表示集合的元素. 集合通常有列举式记法和描述性记法.

例 43

例如 $\mathbb{N} = \{0, 1, 2, \cdots\}$ 是列举法记法,
奇数集合 $= \{a \text{ 为整数} \mid a \equiv 1 \pmod 2\}$ 是描述性记法.

集合族

定义 44

设 I 为一集合且任意 $i \in I$ 都对应一个集合 A_i, 则由这些 A_i $(i \in I)$ 的全体构成的集合称为**集合族**, 通常记为 $\{A_i\}_{i \in I}$, 其中 I 称为该集合族的**下标集合**或**指标集合**.

子集

定义 45

设 A 为一个集合. 如果 a 是 A 中的元素, 则称 a 属于 A, 记为 $a \in A$, 否则记为 $a \notin A$. 如果集合 A 中的每一个元素均是集合 B 中元素, 则称 A 是 B 的**子集** (subset), 即若 $a \in A$, 则 $a \in B$, 记为 $A \subseteq B$ 或 $B \supseteq A$.

- 如果集合 $A \subseteq B$ 且 $B \subseteq A$, 即 $a \in A$ 当且仅当 $a \in B$, 称 A 与 B **相等**, 并记为 $A = B$.
- 如果 $A \subseteq B$ 且 $A \neq B$, 我们称 A 为 B 的**真子集** (proper subset), 记为 $A \subset B$ 或者 $A \subsetneq B$.
- 不含任何元素的集合称为**空集** (empty set), 记为 $\emptyset$. 显然, $\emptyset$ 是任何集合的子集, 且是任何非空集合的真子集.
- 集合 Ω 的所有子集的集合称为 Ω 的**幂集** (power set), 记为 $\mathcal{P}(\Omega)$, 即 $\mathcal{P}(\Omega) = \{A \mid A \subseteq \Omega\}$.

集合的阶

定义 46

如果集合 A 的元素个数有限, 称 A 为**有限集** (finite set), 其元素个数称为集合的**阶**或**基数** (cardinality 或 order of finite set), 记为 $|A|$ 或 $\#A$. 元素个数无限的集合, 即**无限集** (infinite set), 它的阶定义为 ∞. 特别地, 如果 $|A|$ 是有限的, 通常写为 $|A| < \infty$.

集合的交

定义 47

设 A 和 B 是两个集合, 它们的公共元素组成的集合叫做 A 和 B 的**交集** (intersection), 表示成 $A \cap B$, 即

$$A \cap B = \{x \mid x \in A \text{ 且 } x \in B\}.$$

更一般地, 设 $\{A_i\}_{i \in I}$ 为一集合族, 则 A_i $(i \in I)$ 的交为

$$\bigcap_{i \in I} A_i = \{x \mid x \in A_i \text{ 对每个 } i \in I \text{ 成立}\}.$$

集合的并

定义 48

集合 A 与 B 的**并集** (union) 表示成 $A \cup B$, 定义为

$$A \cup B = \{x \mid x \in A \text{ 或 } x \in B\}.$$

更一般地, 设 $\{A_i\}_{i \in I}$ 为一集合族, 则 A_i $(i \in I)$ 的并为

$$\bigcup_{i \in I} A_i = \{x \mid x \in A_i \text{ 对某个 } i \in I \text{ 成立}\}.$$

进一步, 如果 $\{A_i\}_{i \in I}$ 满足对任意 $i \neq j \in I$ 都有 $A_i \cap A_i = \emptyset$, 则称 $\bigcup_{i \in I} A_i$ 为**不交并** (disjoint union), 并记为 $\bigsqcup_{i \in I} A_i$.

集合的差集与补集

定义 49

设 A, B 为某固定集合 Ω 的子集, 则 A 关于 B 的**补集或差集** (complement), 记为 $A - B$ 或 $A \setminus B$, 定义为

$$A - B = \{x \mid x \in A \text{ 且 } x \notin B\}.$$

特别地, 如果所讨论的集合都是固定集合 Ω 的子集, 则 A 关于集合 Ω 的补集通常简称为 A 的补集, 并记为 $\overline{A}$.

集合的直积

定义 50

设 A 和 B 是两个集合, 我们把集合

$$A \times B = \{(a, b) \mid a \in A, b \in B\}$$

叫做 A 与 B 的**直积** (direct product) 或**笛卡尔积** (Cartesian product). 在 $A \times B$ 中, $(a, b) = (a', b')$ 当且仅当 $a = a'$ 且 $b = b'$.

更一般地, 设 $\{A_i\}_{i \in I}$ 为一集合族, 则 A_i $(i \in I)$ 的直积为

$$\prod_{i \in I} A_i = \left\{(a_i)_{i \in I} \mid a_i \in A_i\right\}.$$

集合的映射

定义 51

设 A, B 是两个集合. A 到 B 的一个**映射** (map) f 是一个使得对每个 $a \in A$ 都有唯一一个 $b \in B$ 与之对应的对应法则. 这里 b 叫做 a 在映射 f 之下的**像** (image), a 叫做 b 在 f 下的**原像** (inverse image). 从 A 到 B 的映射 f 记为

$$f : A \to B, \quad a \mapsto f(a),$$

或简记为

$$f : A \to B \text{ 或 } A \xrightarrow{f} B,$$

其中 A 称为映射 f 的**定义域** (domain), $f(A) = \{f(a) \mid a \in A\}$ 称为映射 f 的**像集**或**值域** (codomain).

集合映射

注 51.1

- 当集合 B 是数 (有理数, 实数等) 的集合时, 映射 f 习惯上称为**函数** *(function)*;
- 对任意 $a_1, a_2 \in A$, 当 $f(a_1) = f(a_2)$ 时, 则有 $a_1 = a_2$, 我们称映射 f 为**单射** *(injective)*;
- 如果对任意 $b \in B$, 存在 $a \in A$, 使得 $f(a) = b$, 我们称 f 为**满射** *(surjective)*;
- 如果 f 既是单射, 又是满射, 我们称 f 为**双射** *(bijection)* 或**一一映射** *(one-to-one mapping)*;
- 设 g 也是一个从 A 到 B 的映射, 如果对于任意 $a \in A, f(a) = g(a)$, 称映射 f 与 g 相等, 记为 $f = g$.
- 集合 A 到自身的一个映射称为集合 A 上的一个**变换**. 特别地, 将集合 A 中每个元素均映成其自身的映射

$$1_A : A \to A, 1_A(a) = a.$$

叫做集合 A 的**恒等映射**或恒等变换, 它显然是 A 到 A 的一一对应.

复合映射

定义 52

设 $f : A \to B$ 和 $g : B \to C$ 都是集合之间的映射. 则可经过连续作用, 得到一个从 A 到 C 的映射

$$g \circ f : A \to C, \quad (g \circ f)(a) = g(f(a)).$$

映射 $g \circ f$ 叫做 f 与 g 的**复合映射**或**合成映射**.

- 对映射 $f : A \to B$, 如果存在映射 $g : B \to A$ 使得 $g \circ f = 1_A$ 且 $f \circ g = 1_B$, 则称 f 是**可逆映射**, 称 g 是 f 的**逆映射** (inverse).

结合律

引理 53

设 $f : A \to B$, $g : B \to C$ 和 $h : C \to D$ 为集合间的映射, 则

$$(h \circ g) \circ f = h \circ (g \circ f).$$

- 利用结合律可知, 若 f 可逆, 则其逆映射唯一, 记这个唯一的逆映射为 f^{-1}. 事实上, 设 g_1, g_2 都是 f 的逆映射, 则
$g_1 = g_1 \circ 1_B = g_1 \circ (f \circ g_2) = (g_1 \circ f) \circ g_2 = 1_A \circ g_2 = g_2$.

引理 54

映射 $f : A \to B$ 是一一映射的充分必要条件是 f 是可逆映射.

引理 55

设 $f : A \to B$ 和 $g : B \to C$ 都是一一映射, 则 $g \circ f : A \to C$ 也是一一映射, 并且 $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

集合论悖论

注 55.1

(1) 以上关于集合的陈述使用的是朴素集合语言, 但是朴素集合语言会产生悖论, 如培里悖论 *(1906, G. G. Berry)* 和罗素悖论 *(1902, B. Russell)*, 其中罗素悖论曾经导致了所谓 “第三次数学危机”.

(2) 为解决这些悖论, 人们发展了公理集合论. *Ernst Zermelo (1908)* 和 *Abraham Fraenkel (1922)* 提出了 *Zermelo-Fraenkel* 公理系统 *(ZF*公理*)*, 如果另加选择公理 *(axiom of choice)*, 则称 *ZFC* 公理系统.

无限集合

注 55.2

(1) 关于集合的阶, 前面说的 “元素个数” 也是使用的朴素语言. 设 A, B 是集合. 如果有单射 $f : A \to B$, 我们就说 A 的阶不大于B 的阶, 记作 $|A| \leq |B|$. 果有双射 $f : A \to B$, 我们就说 A 的阶等于 B 的阶, 记作 $|A| = |B|$.

(2) 显然, 当集合 A 和 B 都是有限集时, 则它们阶相等当且仅当它们的元素个数相同. 当 A 是无限集时, 若 $\mathbb{N}$ 到 A 存在一一映射, 我们就称 A 是**可数无限集合** *(countably infinite set)* 或简称 A 是可数的, 否则称 A 为**不可数无限集合** *(uncountably infinite set)* 或简称 A 是不可数的.

(3) 康托 *(Cantor)* 发现 0 与 1 之间的实数集合 $[0, 1]$ 是不可数的, 即 $|\mathbb{N}| < |[0, 1]|$, 从而揭示有本质上不同的 “无限”: 可数的和不可数的, 并且可数的无限是最小的无限.

关系

定义 56

设 S 是一个非空集合, $\mathcal{R}$ 是关于 S 的元素的一个条件. 如果对 S 中任意一个有序元素对 (a, b), 我们总能确定 a 与 b 是否满足条件 $\mathcal{R}$, 就称 $\mathcal{R}$ 是 S 的一个**关系** (relation). 如果 a 与 b 满足条件 $\mathcal{R}$, 则称 a 与 b 有关系 $\mathcal{R}$, 记作 $a\mathcal{R}b$; 否则称 a 与 b 无关系 $\mathcal{R}$. 关系 $\mathcal{R}$ 也称为二元关系.

- 集合的关系可用直积和映射来等价表述.

例

例 57

在整数集 $\mathbb{Z}$ 中, 规定 $a\mathcal{R}b \Leftrightarrow a \mid b$. 因为 $a \mid b$ 与 $a \nmid b$ 有且仅有一个成立, 所以 "$\mid$" 是 $\mathbb{Z}$ 的一个关系. 这个关系具有反身性和传递性.

例 58

在整数集 $\mathbb{Z}$ 中, 规定 $a\mathcal{R}b \Leftrightarrow (a,b) = 1$ (即 a 与 b 互素). 因为 $(a,b) = 1$ 与 $(a,b) \neq 1$ 有且仅有一个成立, 所以互素是 $\mathbb{Z}$ 的一个关系. 这个关系既不满足反身性也不满足传递性, 但却满足所谓的对称性, 即对任意两个整数 a, b, 由 $(a,b) = 1$ 可推出 $(b,a) = 1$.

等价关系

定义 59

设 $\mathcal{R}$ 是非空集合 S 的一个关系, 如果 $\mathcal{R}$ 满足

(1) 反身性, 即对任意的 $a \in S$, 有 $a\mathcal{R}a$;
(2) 对称性, 即若 $a\mathcal{R}b$, 则 $b\mathcal{R}a$;
(3) 传递性, 即若 $a\mathcal{R}b$, 且 $b\mathcal{R}c$, 则 $a\mathcal{R}c$,

则称 $\mathcal{R}$ 是 S 的一个**等价关系** (equivalence relation), 并且如果 $a\mathcal{R}b$, 则称 a 等价于 b, 记作 $a \sim b$.

等价类

定义 60

如果 $\sim$ 是集合 S 的一个等价关系, 对任意 $a \in S$, 令

$$[a] = \{x \in S \mid x \sim a\}.$$

称子集 $[a]$ 为 S 的**一个等价类** (equivalence class). S 的全体等价类的集合称为集合 S 在等价关系下的**商集** (quotient set), 记 $S/\sim$.

例

例 61

易知, 三角形之间的相似是等价关系.

例 62

实数域 $\mathbb{R}$ 上 n 阶方阵之间的相似是等价关系.

例 63

设 m 是任一正整数, 由注 17.1 知 $\mathbb{Z}$ 模 m 的同余是等价关系, 相应的商集为 $\mathbb{Z}$ 模 m 剩余类集 $\mathbb{Z}_m$.

例 64

设 $\{S_i\}_{i\in I}$ 是由某些集合构成的集合族. 在 $\{S_i\}_{i\in I}$ 上定义如下的关系: 对于 $A, B \in \{S_i\}_{i\in I}$, 定义

$$A \sim B \Leftrightarrow \text{存在从 } A \text{ 到 } B \text{ 的一一映射.}$$

容易验证, 这是 $\{S_i\}_{i\in I}$ 上的等价关系 (反身性: $1_A : A \to A$ 是一一映射, 从而 $A \sim A$; 对称性: 若 $f : A \to B$ 是一一映射, 则由引理 54 知 $f^{-1} : B \to A$ 也是一一映射, 从而 $A \sim B \Rightarrow B \sim A$; 由引理 55 立即可得传递性). 对于这种等价关系, 彼此等价的集合叫做是**等势**的. 显然, 两个有限集合等势的充要条件是它们的元素个数相同, 即 $|A| = |B|$. 应当注意的是, 无限集的一个真子集可能会与其自身等势. 例如, 偶整数全体构成的集合与整数之间存在一一映射, 从而它们等势.

等价类的性质

引理 65

如果 $\sim$ 是集合 S 的一个等价关系, 则 S 中每个元素一定在某个等价类中, 并且不同等价类交集为空.

证明: 显然 S 中每个元素一定在某个等价类中.

设 $[a]$ 和 $[b]$ 是 S 的两个等价类. 如果 $[a] \cap [b] \neq \emptyset$, 则有 $c \in [a] \cap [b]$. 于是 $c \sim b, c \sim a$, 从而由对称性知 $b \sim c$, 再由传递性知 $b \sim a$. 又对任意的 $b' \in [b]$, 则 $b' \sim b$, 同样由传递性得 $b' \sim a$. 于是 $b' \in [a]$, 因此 $[b] \subseteq [a]$. 同理可证 $[a] \subseteq [b]$. 于是 $[a] = [b]$. 所以不同的等价类没有公共元素.

分类

定义 66

如果非空集合 S 是它的某些两两不相交的非空子集的并, 则称这些子集为集合 S 的一种**分类**或**分拆** (partition), 其中每个子集称为 S 一个**类** (class). 如果 S 的子集族 $\{S_i\}_{i\in I}$ 构成 S 的一种分类, 则记作 $\mathcal{P}=\{S_i\}_{i\in I}$.

注 66.1

由分类的定义可知, 集合 S 的子集族 $\{S_i\}_{i\in I}$ 构成 S 的一种分类当且仅当:

(1) $S=\bigcup_{i\in I} S_i$;
(2) $S_i\cap S_j=\emptyset, i\neq j$.

(1) 说明 S_i $(i\in I)$ 这些子集无遗漏地包含了 S 的全部元素; *(2)* 说明两个不同的子集无公共元素. 从而 S 的元素属于且仅属于一个子集. 这表明, S 的一个分类必须满足不漏不重的原则.

例

例 67

设 $\mathrm{M}_n(\mathbb{R})$ 为 $\mathbb{R}$ 上全体 n 阶方阵的集合, 令 M_r 表示所有秩为 r 的 n 阶方阵构成的子集, 则有

(1) $\mathrm{M}_n(\mathbb{R}) = \bigcup_{i=0}^{n} M_i$;
(2) $\mathrm{M}_i \cap \mathrm{M}_j = \emptyset, i \neq j$.

所以 $\{\mathrm{M}_i\}_{i\in\{0,1,\cdots,n\}}$ 是 $\mathrm{M}_n(\mathbb{R})$ 的一种分类.

例 68

$\mathbb{Z}_m = \{\bar{a} \mid a = 0, 1, 2, \cdots, m-1\}$ 是整数集 $\mathbb{Z}$ 的一种分类.

例 69

对实数集 $\mathbb{R}$, 令子集 $\mathbb{R}_i = [i, i+1], i \in \mathbb{Z}$. 由于 $i \in \mathbb{R}_i$, 且 $i \in \mathbb{R}_{i-1}$, 同一元素在两个子集中重复出现, 所以 $\{[i, i+1] \mid i \in \mathbb{Z}\}$ 不是 $\mathbb{R}$ 的一种分类.

定理 70

集合 S 的任何一个等价关系都确定了 S 的一种分类, 且其中每一个类都是集合 S 的一个等价类. 反之, 集合 S 的任何一种分类也都给出了集合 S 的一个等价关系, 且相应的等价类就是原分类中的那些类.

证明: 首先, 设为集合 S 的一个等价关系, 则

(1) 对任意的 $a \in S$, 由反身性知 $a \in [a]$, 所以 $S = \bigcup_{a \in S} [a]$.

(2) 根据引理 65 立即可知不同的类没有公共元素, 于是由注 66.1 可得全体等价类形成 S 的一种分类, 显然每一个类都是 S 的等价类.

证明 (续)

其次, 如果已知集合 S 的一种分类 $\mathcal{P}$, 在 S 中规定关系 "$\sim$" :

$$a \sim b \Longleftrightarrow a \text{ 与 } b \text{ 属于同一类}, a, b \in S.$$

对任意的 $a \in S$, 由于 a 属于其本身所在的类, 所以 $a \sim a$. 如果 $a \sim b$, 即 a 与 b 属于同一类, 自然 b 与 a 也属于同一类, 所以 $b \sim a$. 最后, 如果 $a \sim b, b \sim c$, 即 a 与 b 属于同一类, b 与 c 属于同一类, 因而 a 与 c 同在 b 所在的类中, 所以 $a \sim c$. 因此 "$\sim$" 是 S 的一个等价关系. 显然, 由此等价关系得到的等价类就是原分类中的那些类.

例

例 71

设 $S=\{a,b,c\}$, 试确定集合 S 的全部等价关系.

解. 由定理 70 知, 只要求出 S 的全部分类, 即求出 S 的所有可能的子集分划即可.

(1) 如果 S 仅分划为一个子集, 则有 $\mathcal{P}_1=\{S\}$;

(2) 如果 S 仅分划为两个子集, 则有

$$\mathcal{P}_2=\{\{a\},\{b,c\}\},\quad \mathcal{P}_3=\{\{b\},\{a,c\}\},\quad \mathcal{P}_4=\{\{c\},\{a,b\}\}.$$

(3) 如果 S 分划为三个子集, 则有 $\mathcal{P}_5=\{\{a\},\{b\},\{c\}\}$.

解 (续)

因此, 集合 S 共有五个不同的等价关系, 它们是:

$$\sim_1 = \{a \sim a, b \sim b, c \sim c, a \sim b, b \sim a, a \sim c, c \sim a, b \sim c, c \sim b\};$$

$$\sim_2 = \{a \sim a, b \sim b, c \sim c, b \sim c, c \sim b\};$$

$$\sim_3 = \{a \sim a, b \sim b, c \sim c, a \sim c, c \sim a\};$$

$$\sim_4 = \{a \sim a, b \sim b, c \sim c, a \sim b, b \sim a\};$$

$$\sim_5 = \{a \sim a, b \sim b, c \sim c\}.$$