

第三次习题课

助教：林辰，李景荣，赖司贤

主讲人：林辰

知识点拓展（后续会用到相关记号）

- 整除

- 模

- 同余

- 参考资料《初等数论》闵嗣鹤 严士健 编

整除与带余除法

- 定义：设 a, b 是任意两个整数，其中 $b \neq 0$ ，如果存在一个整数 q 使得 $a = bq$ ，我们就说 b 整除 a ，或者 a 被 b 整除，记作 $b|a$

定理 4(带余数除法) 若 a, b 是两个整数,其中 $b > 0$,则存在着两个整数 q 及 r ,使得

$$a = bq + r, 0 \leq r < b \quad (2)$$

成立,而且 q 及 r 是惟一的.

模, 同余

定义 给定一个正整数 m , 把它叫做模. 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 $a \not\equiv b \pmod{m}$.

由定义立刻可以得到下列三个性质:

甲 $a \equiv a \pmod{m}$,

乙 若 $a \equiv b \pmod{m}$, 则 $b \equiv a \pmod{m}$,

丙 若 $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$, 则 $a \equiv c \pmod{m}$.

最大公因数：

■ 最大公因数

- $\gcd(a, b) \stackrel{\text{def}}{=} \max\{d \in \mathbb{Z}^+ | (d|a) \wedge (d|b)\}$
- $a, b \in \mathbb{Z}^+$ 互质 $\Leftrightarrow \gcd(a, b) = 1$, 简记为 $(a, b) = 1$

■ 性质

- $\exists s, t \in \mathbb{Z}^+, \gcd(a, b) = sa + tb$ (线性合成)
- $a < b \rightarrow \gcd(a, b) = \gcd(a, b - a)$ (辗转相减)
- $a > b \rightarrow \gcd(a, b) = \gcd(b, a \bmod b)$ (辗转相除法)

整除与同余

■ 整除

- 整除关系 $| \subseteq \mathbb{Z} \times \mathbb{Z}$, 定义为 $a|b \Leftrightarrow \exists c \in \mathbb{Z}, b = a \times c$
- $(a|b) \wedge (a|c) \rightarrow a|(b+c)$
- $(a|b) \rightarrow a|(b \times c)$
- $(a|b) \wedge (b|c) \rightarrow a|c$

■ 带余除法

- $a \in \mathbb{Z}, d \in \mathbb{Z}^+$, 则 $\exists! q, r \in \mathbb{Z} \wedge 0 \leq r < d$ 使得 $a = d \times q + r$ 。 $r = a \bmod d$
- $(a+b) \bmod d = (a \bmod d + b \bmod d) \bmod d$
- $(a \times b) \bmod d = ((a \bmod d) \times (b \bmod d)) \bmod d$

■ 同余

- 同余关系 $\subseteq \mathbb{Z} \times \mathbb{Z}$, 定义为 $a \equiv b \pmod{m} \Leftrightarrow \exists m \in \mathbb{Z}^+, m|(a-b)$
- “ a 与 b 模 m 同余”

质数：

■ 质数

- 仅含两个平凡正因子的大于1的整数称为质数或者素数，大于1的非质数整数称为和数

■ 算术基本定理

- $\forall n \in \mathbb{Z}^+, n = (p_1)^{\alpha_1} (p_2)^{\alpha_2} \cdots (p_k)^{\alpha_k} (n > 1, p_1 < p_2 < \cdots p_k, \alpha_i \in \mathbb{Z}^+, p_j \text{ 为素数})$
- 此分解唯一

■ 性质

- 有无穷多个素数

Problem Set 4 - Problem 1

证明所有正整数 $n = 4m + 3$ (m 为自然数) 都不能写成两个整数的平方和。

- 考虑同余关系
- 模取几?
- $\text{mod}4$

新的问题

- Problem 1中我们已经证明，模4余3的素数 p 都不能写成两个整数的平方和。
- 那么是否存在模4余1的素数 p ，可以被写成两个整数的平方和？
 - 存在. 例如, $5 = 2^2 + 1^2$, $13 = 2^2 + 3^2$, $17 = 1^2 + 4^2$ 等等
- 对于所有模4余1的素数 p ，都可以被写成两个整数的平方和吗？

Problem Set 4 - Problem 2

证明方程 $x^2 + y^2 = z^2$ 有无穷多组正整数解 $\langle x, y, z \rangle$

- 勾股数，毕达哥拉斯三元组
- 观察—找合适的形式（完全平方公式）

Problem Set 4 - Problem 2

证明方程 $x^2 + y^2 = z^2$ 有无穷多组正整数解 (x, y, z)

■ 错误解法：

(反证法) 假设有有限组解，

则对每一组解 (x, y, z) 计算 $x+y+z$ 。



取其中和最大的一组解，记为 (a, b, c)

不难证明对于大于1的正整数 n ， (na, nb, nc) 也为一组解

但 $na+nb+nc > a+b+c$ ，与 (a, b, c) 为和最大的解矛盾

假设不成立，

因此有无穷多组解。

方程有有限组解
的反面是什么？

Problem Set 4 - Problem 2 (改)

给出方程 $x^2 + y^2 = z^2$ (1) 所有正整数解 $\langle x, y, z \rangle$

■ 奇偶性探路

引理 不定方程

$$uv = w^2, w > 0, u > 0, v > 0, (u, v) = 1 \quad (2)$$

的一切正整数解可以写成公式:

$$u = a^2, v = b^2, w = ab, a > 0, b > 0, (a, b) = 1. \quad (3)$$

Problem Set 4 - Problem 2 (改)

给出方程 $x^2 + y^2 = z^2$ (1) 所有正整数解 $\langle x, y, z \rangle$

引理 不定方程

$$uv = w^2, w > 0, u > 0, v > 0, (u, v) = 1 \quad (2)$$

的一切正整数解可以写成公式:

$$u = a^2, v = b^2, w = ab, a > 0, b > 0, (a, b) = 1. \quad (3)$$

定理 1 不定方程(1)的适合条件

$$x > 0, y > 0, z > 0, (x, y) = 1, 2 \nmid x \quad (4)$$

的一切正整数解可以用下列公式表出来:

$$\begin{aligned} x &= 2ab, y = a^2 - b^2, z = a^2 + b^2, \\ a &> b > 0, (a, b) = 1, a, b \text{ 一奇一偶}. \end{aligned} \quad (5)$$

Problem Set 4 - Problem 2 (改)

给出方程 $x^2 + y^2 = z^2$ (1) 所有正整数解 $\langle x, y, z \rangle$

定理 1 不定方程(1)的适合条件

$$x > 0, y > 0, z > 0, (x, y) = 1, 2 \mid x \quad (4)$$

的一切正整数解可以用下列公式表出来:

$$\begin{aligned} x &= 2ab, y = a^2 - b^2, z = a^2 + b^2, \\ a &> b > 0, (a, b) = 1, a, b \text{ 一奇一偶}. \end{aligned} \quad (5)$$

推论 1.1 单位圆周上的一切有理点可以表成

$$\left(\pm \frac{2ab}{a^2 + b^2}, \pm \frac{a^2 - b^2}{a^2 + b^2} \right) \text{ 及 } \left(\pm \frac{a^2 - b^2}{a^2 + b^2}, \pm \frac{2ab}{a^2 + b^2} \right),$$

其中 a, b 不全为 0, \pm 号可以任意取.

Problem Set 4 - Problem 4

用反证法证明：不存在有理数 r 使得 $r^3 + r + 1 = 0$.

- 假设存在有理数 $r = \frac{p}{q}$, 其中 p, q 为整数且 $\gcd(p, q) = 1$.
- 则原方程可以化为 $p^3 + pq^2 + q^3 = 0$.
- 观察两边奇偶性

Problem Set 4 - Problem 5

在黑板上写下数字 $1, 2, 3 \dots 2n$, 其中 n 是奇数。从中任意挑出两个数 j 和 k , 在黑板上写下 $|j - k|$ 并擦掉 j 和 k 。继续这个过程, 直到黑板上只剩下一个整数为止。证明这个整数必为奇数。

- 考虑所有数字的和
- 考虑奇数偶数的个数

Problem Set 4 - Problem 6

有一个 $n \times n$ 的方格表，先允许从中任意选择 $n - 1$ 个方格涂为黑色，然后再逐步地将那些至少与两个已涂黑的方格相邻的方格也涂为黑色。试证明：不论怎样选择最初的 $n - 1$ 个格，都不能按这样的法则涂黑所有的方格。

- 考虑周长
- 逐步涂黑方块的过程总周长不会增加
- $n-1$ 个黑色方块总周长？
- 全部涂黑后方格表的总周长？

Problem Set 4 - Problem 7

证明任一个有理数 x 和任一个无理数 y 之间都有一个无理数。

- “不妨设” $x > y$ 还是 “设” $x > y$
- 中间的无理数是谁?
- 取 $x + \frac{y-x}{\sqrt{2}}$ 可以吗?
- 改：证明任一个有理数 x 和任一个无理数 y 之间都有一个有理数

Problem Set 4 - Problem 8

- a) 证明或驳斥如果 a 和 b 是有理数, 那么 a^b 也是有理数。
- b) 是否存在有理数 x 和无理数 y , 使得 x^y 是无理数。
- c) 是否存在无理数 x 和 y , 使得 x^y 是有理数。

■ 举例

■ 注意: 你必须清楚所取的数确实是个有理数/无理数 (证明之)

知识点回顾

- 集合论
- 二元关系

集合论

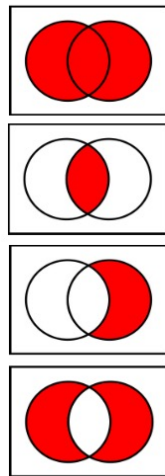
- 集合没有明确的定义。通常用大写字母表示集合，如 A 、 B 、 C 等，用小写字母表示元素，如 a 、 b 、 c 等。若集合 A 系由 a 、 b 、 c 等诸元素所组成，则表如 $A = \{a, b, c, \dots\}$ ，而 a 为 A 之元素，亦常用 $a \in A$ 之记号表之者， a 非 A 之元素，则记如 $a \notin A$ 。”
- A 为 B 之子集（记为 $A \subseteq B$ ）指 $\forall x(x \in A \rightarrow x \in B)$ ， A 为 B 之真子集（记为 $A \subset B$ ）指 $A \subseteq B$ 且 $A \neq B$ 。
- $A = B \iff (A \subseteq B \wedge B \subseteq A)$

集合论

- 证明：如果 $X \subseteq Y$ 且 $Y \subseteq Z$, 则 $X \subseteq Z$
- 要证明：“对任意的 a , 如果 $a \in X$, 则 $a \in Z$ ”
- 证明：
 - 对任意的 $a \in X$
 - 根据已知的 “ $X \subseteq Y$ ”, 可得: $a \in Y$
 - 根据已知的 “ $Y \subseteq Z$ ”, 可得: $a \in Z$
 - 所以, $\forall a (a \in X \rightarrow a \in Z)$, 即 $X \subseteq Z$

集合论

- 空集本身是一个集合，也可以做为另一个集合的元素或者子集： $\emptyset \in \{\emptyset\}$ ， $\emptyset \subseteq \{\emptyset\}$ ，但因为空集不含任何元素，故 $\emptyset \notin \emptyset$ ， $\emptyset \neq \{\emptyset\}$
- 集合 A 的幂集 $P(A) = \{x | x \subseteq A\}$ ，即由集合 A 的全体子集构成的集合
- 集合的运算：
 - 集合的并： $A \cup B = \{x | x \in A \vee x \in B\}$
 - 集合的交： $A \cap B = \{x | x \in A \wedge x \in B\}$
 - 集合的相对补： $A - B = \{x | x \in A \wedge x \notin B\}$
 - 集合的对称差： $A \oplus B = \{x | (x \in A \wedge x \notin B) \vee (x \in B \wedge x \notin A)\}$
 $= (A - B) \cup (B - A)$



集合论

■ 例：判断下列语句是真还是假

- $x \in \{x\}$ T
- $\{x\} \subseteq \{x\}$ T
- $\{x\} \in \{x\}$ F
- $\{x\} \in \{\{x\}\}$ T
- $\emptyset \subseteq \{x\}$ T
- $\emptyset \in \{x\}$ F

集合论

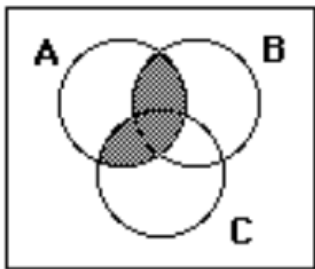
■ 集合代数:

- 交换律: $A \cup B = B \cup A, A \cap B = B \cap A$
- 结合律: $A \cup (B \cup C) = (A \cup B) \cup C, A \cap (B \cap C) = (A \cap B) \cap C$
- 分配律: $A \cup (B \cap C) = (A \cup B) \cap (A \cup C), A \cap (B \cup C) = (A \cap B) \cup (A \cap C)$
- 吸收律: $A \cup (A \cap B) = A, A \cap (A \cup B) = A$
- 幂等律: $A \cap A = A \cup A = A$
- De Morgan 律: $A - (B \cup C) = (A - B) \cap (A - C), A - (B \cap C) = (A - B) \cup (A - C)$
- 空集性质: $A \cap \emptyset = \emptyset, A \cup \emptyset = A$
- 幂集性质: $P(A \cap B) = P(A) \cap P(B), P(A \cup B) \supseteq P(A) \cup P(B)$

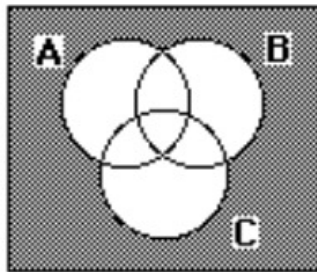
集合论

■ 例：画出以下集合 A、B、C 的每个组合的文氏图：

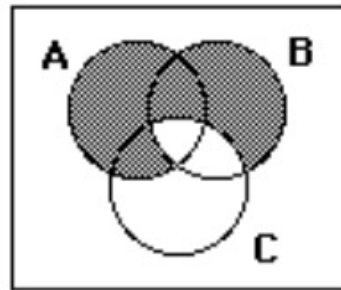
- a) $A \cap (B \cup C)$
- b) $\bar{A} \cap \bar{B} \cap \bar{C}$
- c) $(A - B) \cup (A - C) \cup (B - C)$



(a)



(b)



(c)

Problem 1

设集合 a, b, c 各不相同，试判定下列命题的真假.

(a) $\emptyset \in \{\emptyset\}$

(b) $\{\{a, b\}, c, \emptyset\} = \{\{a, b\}, c\}$

(c) $\{\emptyset\} \in \{\emptyset\}$

(d) $\{\{a\}, \{b\}\} = \{\{a, b\}\}$

(e) $\{\emptyset\} \subset \{\emptyset, \{\emptyset\}\}$

(f) $\{\emptyset, \{\emptyset\}, a, b\} = \{\{\emptyset, \{\emptyset\}\}, a, b\}$

■ 注意区分元素、集合、子集三个概念！

Problem 2

试判断下列各集合是否为某个集合的幂集.

(a) \emptyset

(b) $\{\emptyset, \{a\}\}$

(c) $\{\emptyset, \{a\}, \{\emptyset, a\}\}$

(d) $\{\emptyset, \{a\}, \{b\}, \{a, b\}\}$

- 集合A的幂集是集合A的全体子集构成的集合（注意不要遗漏空集！）

Problem 3

试求满足下列谓词的集合，设论域为整数集.

(a) $P(x) : x^2 < 3$

(b) $Q(x) : x^2 > x$

(c) $R(x) : x^2 = 3$

■ 注意论域为整数集

Problem 4

令 A, B, C 为集合，证明或者否定以下集合等式的成立：

a) $(A \cup B \cup C) - (A \cup B) = C$

b) $A - (B - C) = (A - B) - (A - C)$

- 文氏图探路
- 严谨证明或给出反例

Problem 5

若集合分别 A 、 B 、 C 满足下列条件，能否断言 $A = B$?，请说明理由或者给出反例.

(a) $A \cup C = B \cup C$

(b) $A \cap C = B \cap C$

(c) $A \cup C = B \cup C$ 并且 $A \cap C = B \cap C$

- 文氏图
- 严谨证明或给出反例

Problem 6

令 A 和 B 为全集 U 的子集. 证明 $A \subseteq B$ 当且仅当 $\overline{B} \subseteq \overline{A}$, 这里 \overline{A} 指绝对补集 $U - A$.

- “当且仅当”
- 文氏图探路
- 严谨证明

Problem 7

令集合 A, B 是全集 U 的子集，证明如下等式成立：

a) $A \oplus A = \emptyset$

b) $A \oplus U = \overline{A}$

c) $(A \oplus B) \oplus B = A$

■ 文氏图探路

■ 左包含右，右包含左（一侧的任意元素属于另一侧）

Problem 8

令 $A_i = \{\cdots, -2, -1, 0, 1, \cdots, i\}$, 试求:

(a) $\bigcup_{i=1}^n A_i$

(b) $\bigcap_{i=1}^n A_i$

■ 交集、并集的定义

■ n 换成 ∞ ?

Problem 9

试求下列集合之后继.

(a) $\{1, 2, 3\}$

(b) \emptyset

(c) $\{\emptyset\}$

(d) $\{\emptyset, \{\emptyset\}\}$

■ 集合 A 的后继是集合 $A \cup \{A\}$ 。

Problem 10

令 A, B, C 为集合，试证明： $A \cup B \cup C = (A - B) \cup (B - C) \cup (C - A) \cup (A \cap B \cap C)$ 。

- 文氏图探路
- 左包含右，右包含左（一侧的任意元素属于另一侧）
- 成员表

Thanks for listening

- Q & A