组合数学第 13 讲

授课时间: 2024 年 11 月 25 日 授课教师: 孙晓明 记录人: 张育瑞 祝立言

1 抽屉原理（鸽笼原理）

定理 1 (抽屉原理)**.** 将至少 $n+1$ 个物体放入 n 个抽屉中，则一定存在一个抽屉里装有至少 2 个物体；将至多 $n-1$ 个物体放入 n 个抽屉中，则一定存在一个抽屉为空.

推论 2. m,n 为正整数，将至少 $mn+1$ 个物体放入 n 个抽屉中，则一定存在一个抽屉里装有至少 $m+1$ 个物体.

证明 使用反证法：假设每个抽屉里都只装了不超过 m 个物体，则至多会有 mn 个物体，这与命题中至少有 $mn+1$ 个物体这一条件矛盾，证毕. □

推论 3. m,n 为正整数，将至多 $mn-1$ 个物体放入 n 个抽屉中，则一定存在一个抽屉里装有至多 $m-1$ 个物体.

证明 使用反证法：假设每个抽屉里都装至少 m 个物体，则至少会有 mn 个物体，这与命题中至多有 $mn-1$ 个物体这一条件矛盾，证毕. □

2 二平方和问题

在这一节，我们探究正整数 n 满足什么条件时，可以写成两个整数的平方和，即 $\exists\, x,y\in\mathbb{N}, n=x^2+y^2$.

引理 4 (Fermat 二平方和定理)**.** 奇素数 p 可以表示为两个整数的平方和的充分必要条件是 $p\equiv 1 \pmod 4$.

证明 这里只证明充分性, 必要性在推广的费马平方和定理中证明. 因为 $p\equiv 1 \pmod 4$，由 Euler 判别定理，

$$\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}}=1 \pmod p.$$

所以 $\exists\, z\in\mathbb{N}$，使得 $z^2\equiv -1 \pmod p$.

对于所有满足 $0\le i,j\le\lfloor\sqrt{p}\rfloor$ 的数对 (i,j)，考虑 $i+zj$. 由乘法原理，符合条件的数对个数为 $\left(\lfloor\sqrt{p}\rfloor+1\right)^2>\sqrt{p}^2=p$. 而模 p 剩余类中只有 p 个元素，由抽屉原理，存在 $(i_1,j_1)\neq(i_2,j_2)$ 使得

$$i_1+zj_1\equiv i_2+zj_2 \pmod p.$$

所以

$$\begin{aligned}(i_1-i_2)^2\equiv z^2(j_2-j_1)^2\equiv -1\times(j_2-j_1)^2 \pmod p,\\ (i_1-i_2)^2+(j_2-j_1)^2\equiv 0 \pmod p.\end{aligned}$$

因为 $(i_1,j_1)\neq(i_2,j_2)$, 所以 $(i_1-i_2)^2+(j_2-j_1)^2\neq 0$; 又因为 $0\le i_1,i_2,j_1,j_2\le\lfloor\sqrt{p}\rfloor$, 所以 $(i_1-i_2)^2+(j_2-j_1)^2<2\lfloor\sqrt{p}\rfloor^2\le 2p$. 于是由 $(i_1-i_2)^2+(j_2-j_1)^2\equiv 0 \pmod p$ 可以直接得出 $(i_1-i_2)^2+(j_2-j_1)^2=p$，即 p 可以表示为两个整数的平方和. □

引理 5. *若 $n, n_1, n_2 \in \mathbb{N}$，且 $n = n_1 n_2$，$n_1 = x_1^2 + y_1^2, n_2 = x_2^2 + y_2^2$，其中 $x_1, y_1, x_2, y_2 \in \mathbb{N}$，则 $\exists x, y \in \mathbb{N}$，使得 $n = x^2 + y^2$.*

证明 直接对 n 进行如下计算即可.

$$\begin{aligned} n &= n_1 n_2 \\ &= (x_1^2 + y_1^2)(x_2^2 + y_2^2) \\ &= (x_1 x_2 - y_1 y_2)^2 + (x_1 y_2 + x_2 y_1)^2. \end{aligned}$$

□

定理 6 (推广的 Fermat 二平方和定理)**.** *n 是正整数，且其素因数分解为：*

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

则 n 可以表示为两个整数的平方和的充分必要条件是对于所有满足 $p_i \equiv 3 \pmod 4$ 的素数 p_i，其对应的指数 α_i 都是偶数.

证明 先证明充分性. 我们可以将 n 的所有素因子分成三类：2、$4k+1$ 型素数和 $4k+3$ 型素数. 由条件可知 n 的 $4k+3$ 型素数对应的指数都是偶数，于是 n 的素因数分解可以改写成

$$\begin{aligned} n &= 2^{\gamma} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} q_1^{2\beta_1} q_2^{2\beta_2} \cdots q_t^{2\beta_t} \\ &= 2^{\gamma} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} (q_1^2)^{\beta_1} (q_2^2)^{\beta_2} \cdots (q_t^2)^{2\beta_t}. \end{aligned}$$

其中 $\{p_1, p_2, \ldots, p_s\}$ 为 n 的所有 $4k+1$ 型素数；$\{q_1, q_2, \ldots, q_t\}$ 为 n 的所有 $4k+3$ 型素数. $2 = 1^2 + 1^2$，$q_i^2 = q_i^2 + 0^2$，由引理 4，p_i 可以表示为两个整数的平方和，所以 n 是若干个可以表示为两个整数的平方和的整数的乘积，再由引理 5，得出 n 可以表示为两个整数的平方和.

以下证明必要性. 使用反证法. 不妨设 q 为 n 的一个素因子，$q \equiv 3 \pmod 4$，且 n 中 q 因子的次数为正奇数. n 可以写成两个整数的平方和，设 $n = x^2 + y^2$，$x, y \in \mathbb{N}$. 则 $p_1 \mid x^2 + y^2$. 即

$$\begin{aligned} x^2 + y^2 &\equiv 0 \pmod{p_1}, \\ x^2 &\equiv -y^2 \pmod{p_1}. \end{aligned}$$

若 $q \nmid y$，在模 q 的剩余类中，$\exists y^* \in \mathbb{N}$，使得 $y^* y \equiv 1 \pmod q$. 所以

$$(xy^*)^2 = x^2 y^{*2} \equiv -(yy^*)^2 \equiv -1 \pmod q.$$

因为 $q \equiv 3 \pmod 4$，由 Euler 判别定理，

$$\left(\frac{-1}{q}\right) \equiv (-1)^{\frac{q-1}{2}} = -1 \pmod q.$$

即 -1 不是 q 的二次剩余，这与上式矛盾.

若 $q \mid y$. 易得 $q \mid x$. 令 m 为 x 和 y 的最大公约数中 q 因子的次数，即 $x = x_0 q^m, y = y_0 q^m$ 且 $x_0 \nmid q$ 或 $y_0 \nmid q$. 于是 $n = x^2 + y^2 = q^{2m}(x_0^2 + y_0^2)$，所以 $\frac{n}{q^{2m}} = x_0^2 + y_0^2$，因为 n 中 q 因子的次数为奇数，所以 $\frac{n}{q^{2m}}$ 中 q 因子的次数仍然为奇数且有 $q \nmid x_0$ 或 $q \nmid y_0$，余下分析便与 $q \nmid y$ 时的分析无异了，所以依然可以推出矛盾.

□

3 抽屉原理例题

例 1 集合 $S \subseteq \{1, 2, \ldots, 100\}$, 且 $|S| = 51$，则存在 $a, b \in S$，使得 a 与 b 互素.

证明 构造抽屉：$\{1, 2\}, \{3, 4\}, \{5, 6\}, \ldots, \{99, 100\}$，共有 50 个抽屉. 由抽屉原理，$S$ 中必有两个元素在同一个抽屉中，因为两个相邻正整数一定互素，所以 S 中在同一个抽屉中的两个元素必然互素. □

讨论：在这一例中，若 $|S| = 50$，取 $S = \{2, 4, 6, \ldots, 96, 98, 100\}$，则 S 中任意两个数均不互素，所以为了保证一定存在 $a, b \in S$，使得 a 与 b 互素，$|S|$ 的最小值就是 *51*.

例 2 集合 $S \subseteq \{1, 2, \ldots, 100\}$, 且 $|S| = 51$，则存在不同的 $a, b \in S$，使得 $a \mid b$.

证明 对于 $1 \leq i \leq 50$，构造抽屉 $A_i = \{(2i-1)2^t \mid 1 \leq (2i-1)2^t \leq 100\}$. 1 到 100 中的每个整数都在其中一个抽屉中，共有 50 个抽屉. 由抽屉原理，S 中必有两个元素在同一个抽屉中，因为在同一个抽屉里任取两个不同的数都有倍数关系，所以 S 中在同一个抽屉中的两个不同元素必然有倍数关系. □

讨论：在这一例中，若 $|S| = 50$，取 $S = \{51, 52, 53, \ldots, 98, 99, 100\}$，则 S 中任意两个不同的数均没有倍数关系，所以为了保证一定存在不同的 $a, b \in S$，使得 $a \mid b$，$|S|$ 的最小值就是 *51*.

例 3 小明是一名国科大的学生，他正在备考英语考试，现在距离考试还有 11 周时间，他开始背单词，假设他每天至少背 1 页单词，每周最多背 12 页单词. 请证明：一定存在连续的若干天，小明在这些天正好背了 21 页单词.

证明 11 周共 77 天. 记 a_i 为小明第 i 天背单词的页数，$S_i = \sum_{k=1}^{i} a_k$ 为前 i 天背单词的页数. 由题目条件可知，小明在这 11 周里，每周背单词页数都不超过 12 页，所以 $S_{77} \leq 12 \cdot 11 = 132$，又因为 $a_i \geq 1$，所以

$$1 \leq S_1 < S_2 < S_3 < \ldots < S_{77} \leq 12 \cdot 11 = 132.$$

将该不等式的所有项加 21，得到

$$S_1 + 21 < S_2 + 21 < \ldots < S_{77} + 21 \leq 132 + 21 = 153.$$

所有 $\{S_i\}$ 和 $\{S_i + 21\}$，共 $77 \times 2 = 154$ 个正整数都在 1 到 153 的范围之中，由抽屉原理，这 154 个正整数中必有两数相等，又因为 $\{S_i\}$ 和 $\{S_i + 21\}$ 都是严格单调增的数列，所以其中相等的两数必然分别来自不同集合，不妨设 $S_j = S_i + 21$，这说明小明从第 $i + 1$ 天到第 j 天正好背了 21 页单词，证毕. □

讨论：将上例中的 *21* 改成更小的正整数，使用上述方法依然可以证明结论成立. 我们来看如何将其换成更大的正整数：如果我们将 *21* 换成 *77*，对于

$$1 \leq S_1 < S_2 < S_3 < \ldots < S_{77} \leq 132,$$

考虑 $S_1, S_2 \ldots S_{77}$ 模 *77* 的余数，若有某个 $S_i \equiv 0 \pmod{77}$，那么直接就有 $S_i = 77$；否则，模 *77* 的剩余类除了 *0* 以外还有 *76* 个元素，由抽屉原理，$S_1, S_2 \ldots S_{77}$ 中必有两个元素 S_i, S_j 模 *77* 同余，不妨设 $i < j$. 因为它们不相等且均不大于 *132*，所以一定相差 *77*，我们进而得到小明从第 $i + 1$ 天到第 j 天正好背了 *77* 页单词. 将 *77* 换成 *67* 到 *76* 之间的任何一个正整数，用上述方法依然可以证明结论成立.

对于某个 $22 \leq i \leq 66$ 或 $i \geq 78$，我们是否还能保证一定存在连续的若干天，小明在这些天正好背了 i 页单词？此问题留作思考.

例 4 有 10 个人，每个人的年龄在 1 到 100 之间，请证明：在这 10 个人中一定存在两组人（1 个人也可以单独成为一组），第一组人的年龄之和与第二组人的年龄之和相等，且这两组人交集为空.

证明 我们将这 10 个人的年龄分别记为 $a_1, a_2, \ldots, a_{10}$. $\{a_1, a_2, \ldots, a_{10}\}$ 共有 $2^{10} = 1024$ 个子集，把空集去掉之后还剩下 1023 个子集（这里相同的年龄仍然记作不同的元素）. 对于每个子集，其元素和至少为 1，至多为 $10 \times 100 = 1000$，由抽屉原理，一定有两个不同的子集 A 和 B，它们的元素和相等，因为同时去掉共有的元素依然可以保证元素和相等，所以 $A\backslash B$ 和 $B\backslash A$ 即为满足条件的两组人. □

讨论：如果现在只有 *9* 个人（甚至更少），上述结论是否还会成立呢？更一般地，如果将数字限定在 *1* 到 n 之间，至少需要多少个人才可以保证存在年龄之和相同的两组人呢？该问题经常以如下的形式出现：在 $\{1, 2, \ldots, n\}$ 中最多能够取出一个多大的子集 S，使得 S 的任何两个子集都具有不同的元素和？

4 选做题

在 $\{1, 2, \ldots, n\}$ 中至少取多少个数，才能保证其中存在三个数两两互素？如果要求存在更多的数两两互素呢?