组合数学第十四讲

授课时间: 2018 年 12 月 24 日　授课教师: 孙晓明　　记录人: 李颖彦　李昊宸

1　ax^2+by^2 型素数

定理 1. *对于任意奇素数 p，存在正整数 x，y 使得 $p=x^2+y^2$ 当且仅当 p 为 4k+1 型*

证明　一方面，对于 4k+3 型素数，采取反证法，假设存在 x,y，使得 $p=x^2+y^2$, 所以 $x^2 \equiv -y^2 \pmod p$, 将 y 取逆得，$(xy^{-1})^2 \equiv -1 \pmod p$，但对于 4k+3 型素数，-1 是非二次剩余，矛盾。

另一方面，因为 -1 是 4k+1 型素数的二次剩余，故存在正整数 z 满足 $z^2 \equiv -1 \pmod p$, 考虑集合 $S=\{a+b\cdot z|0\le a,b\le[\sqrt{p}]\}$, 集合的势 $|S|=([\sqrt{p}]+1)^2>p$，所以根据鸽巢原理，必定存在 a_1,b_1,a_2,b_2, 使得

$$a_1+b_1z\equiv a_2+b_2z \pmod p$$

移项可得 $(a_1-a_2)^2\equiv(b_1-b_2)^2(-1) \pmod p$, 所以

$$p|(a_1-a_2)^2+(b_1-b_2)^2\le([\sqrt{p}])^2+([\sqrt{p}])^2<2p$$

所以 $x^2+y^2=p$，得证 □

定理 2. *对于任意奇素数 p，存在正整数 x，y 使得 $p=x^2+2y^2$ 当且仅当 p 为 $8k+1$ 型或 $8k+3$ 型*

证明　一方面，$p=x^2+2y^2$，则 $x^2\equiv-2y^2 \pmod p$, 将 y 取逆得 $(xy^{-1})^2\equiv-2 \pmod p$, 所以 $(\dfrac{-2}{p})=1$

结合以前课所学的 $(\dfrac{-1}{p})$ 的性质可得：

$$(\frac{-1}{p})(\frac{-2}{p})=\begin{cases}1, & 8k+1,\\ 1, & 8k+3,\\ -1, & 8k+5,\\ -1, & 8k+7,\end{cases}$$

推出 $p=8k+1,8k+3$

另一方面，因为 $(\dfrac{-2}{p})=1$, 所以设 $z^2\equiv-2 \pmod p$, 考虑集合 $S=\{a+b\cdot z|0\le a,b\le[\sqrt{p}]\}$, 集合的势 $|S|=([\sqrt{p}]+1)^2>p$，所以根据鸽巢原理，必定存在 a_1,b_1,a_2,b_2, 使得

$$a_1+b_1z\equiv a_2+b_2z \pmod p$$

移项可得 $(a_1-a_2)^2\equiv(b_1-b_2)^2(-2) \pmod p$, 所以

$$p|(a_1-a_2)^2+2(b_1-b_2)^2\le([\sqrt{p}])^2+2([\sqrt{p}])^2<3p$$

所以 $x^2+y^2=p$ 或 $2p$，若等于 p，得证。
若等于 2p, 因为 $x^2+2y^2=2p$, 而 2p 与 $2y^2$ 均为偶数, 所以 x^2 为偶数，即 $2|x$，设 $x=2\tilde{x}$, 代入得 $4\tilde{x}^2+2y^2=2p$, 即 $y^2+2\tilde{x}^2=p$, 得证。

□

选做题: 考虑 p 为奇素数，存在正整数 x，y 使得 $p=x^2+3y^2$ 的充分必要条件。

命题 3 (鸽巢原理的应用). *$\forall a_1,a_2,...,a_{100}\in\mathbb{Z}$, 必定存在部分和 $a_{i_1}+...+a_{i_k}$ 被 100 整除*

证明 定义 $S_1=a_1, S_2=a_1+a_2, ..., S_{100}=a_1+...+a_{100}$ 以 mod 100 后的余数来对 S_i 分类，有 0，1，...，99 这 100 种情况，若有 $S_i\equiv 0 \pmod{100}$, 则成立。
否则，根据鸽巢原理，必定 $\exists i\le j, \exists 1\le k\le 99, s.t.$ 同时有 $S_i, S_j\equiv k \pmod{100}$, 则有 $100|S_i-S_j$, 得证。

□

在介绍要讲定理之前，我们先看几个个例子：
例 1 问正整数 k 至少是多少，能使得任取 k 个数，从中必定能选出 2 个数 a_{i_1}, a_{i_2}，满足 $2|a_{i_1}+a_{i_2}$。

证明 答案是 k=3，此时对将这任意 3 个正整数 mod2，根据鸽巢原理，至少有 2 个数的余数相等，此时无论余数是 0 还是 1，将这两个数相加，都将使得他们的和 mod2 余 0；而 k=2 时，取 mod2 余数分别为 0 和 1 的两个数，显然矛盾。 □

例 2 问正整数 k 至少是多少，能使得任取 k 个数，从中必定能选出 3 个数 $a_{i_1}, a_{i_2}, a_{i_3}$，满足 $3|a_{i_1}+a_{i_2}+a_{i_3}$。

证明 答案是 k=5，此时对将这任意 5 个正整数 mod3，分类讨论：
1. 若有至少 3 个数在一个同余类中，直接得证。
2. 否则，根据鸽巢原理，数在同余类中的分布为 1，2，2。此时分别在余数为 0，1，2 的同余类中中各取一个数，这三个数之和满足条件。
而 k=4 时，取 2 个 mod3 余数为 1 和两个 mod3 余数为 2 的数，不成立。 □

例 3 问正整数 k 至少是多少，能使得任取 k 个数，从中必定能选出 4 个数 $a_{i_1}, a_{i_2}, a_{i_3}\ a_{i_4}$，满足 $3|a_{i_1}+a_{i_2}+a_{i_3}+a_{i_4}$。

证明 答案是 k=7. 运用 n=2 时的结论，则任意取 7 个数，在其中任意取 3 个数，可以找到 2 个数之和被 2 整除，如此循环 3 次，则可以找到 3 对数 $(a_1,a_2),(a_3,a_4),(a_5,a_6)$，每对数的和都能被 2 整除。将这每对和除以 2, 得到三个整数 $\frac{a_1+a_2}{2}, \frac{a_3+a_4}{2}, \frac{a_5+a_6}{2}$，再一次运用 n=2 时的结论，则其中必有两个数，满足 $2|\frac{a_{i_1}+a_{i_2}}{2}+\frac{a_{i_3}+a_{i_4}}{2}$, 此时这 4 个数 $a_{i_1}\ a_{i_2}\ a_{i_3}\ a_{i_4}$ 即满足要求的数。
k=6 时，取 3 个 mod4 余数为 0 和 3 个 mod4 余数为 1 的数，不成立。 □

2 Erdös-Ginzburg-Ziv 定理

定理（Erdös-Ginzburg-Ziv） 对于任意的素数 p，任取 2p−1 个整数，从中必定能选出 p 个整数 $a_{i1}, a_{i2}, \cdots, a_{ip}$，其中 i1<i2<⋯<ip，满足 $p\mid\sum_{k=1}^{p}a_{ik}$

第一种证明：对于该定理的证明，我们对结论使用反证法：

假设对于任意的 p 个整数 $a_{i1},a_{i2},\cdots,a_{ip}$，都有 $p\nmid\sum_{k=1}^{p}a_{ik}$，那么 p 与 $\sum_{k=1}^{p}a_{ik}$ 互素，

由费马小定理，$(a_{i1}+a_{i2}+...+a_{ip})^{p-1}\equiv 1(\bmod p)$，

于是 $\sum_{1\le i1<i2<\ldots<ip\le 2p-1}(a_{i1}+a_{i2}+...+a_{ip})^{p-1}\equiv\binom{2p-1}{p}\equiv\frac{(2p-1)!}{p!(p-1)!}(\bmod p)$ 因为分子和分母上均只含有一个 p 因子，故 $p\nmid\binom{2p-1}{p}$。下面考虑等式左边：

$$
\begin{aligned}
\text{左边} &= \sum_{1\le i1<i2<\ldots<ip\le 2p-1}\ \sum_{\alpha_1+\ldots+\alpha_p=p-1}a_{i1}^{\alpha_1}a_{i2}^{\alpha_2}\cdots a_{ip}^{\alpha_p}\frac{(p-1)!}{\alpha_1!\alpha_2!..\alpha_p!}\\
&=\sum_{s}\ \sum_{1\le i1<i2<\ldots<is\le 2p-1}\ \sum_{\substack{\beta_1+\ldots+\beta_s=p-1\\ \beta_i\ge 1}}a_{i1}^{\beta_1}a_{i2}^{\beta_2}\cdots a_{is}^{\beta_s}\frac{(p-1)!}{\beta_1!\beta_2!..\beta_s!}\binom{2p-1-s}{p-s}
\end{aligned}
$$

这是因为从 2p-1 中取出 p 原集，且一定包含 $i_1,i_2,\cdots,i_s$ 这 s 个元素的种类有 $\binom{2p-s-1}{p-s}$ 种，

并且 $\binom{2p-s-1}{p-s}=\frac{(2p-1-s)!}{(p-s)!(p-1)!}$，分子有一个素因子 p，分母没有，故 $p\mid\binom{2p-s-1}{p-s}$，

从而 p 整除等式左边，这与 p 不整除等式右边矛盾！ Q.E.D

下面我们考虑另一种证明方法。

对于两个整数集 A 和 B，定义集合的加法 $A+B=\{a+b\mid a\in A,b\in B\}$，自然的，有 $|A+B|\ge|A|+|B|-1$。感兴趣的同学可课下自证。那么，我们引入以下结论：

引理(Cauthy-Davenport) 对于剩余类环 Z_p 中元素的两个子集 A 和 B，定义 $A+B=\{a+b(\bmod p)\mid a\in A,b\in B\}$，那么有 $|A+B|\ge\min\{|A|+|B|-1,p\}$

在这里我们给出 $|B|=2$ 的**证明**，即 $|A+B|\ge|A|+1$：

设 $B=\{a,b\}$，构建关于 A 的陪集 $A'=a+A$。假设 $|A+B|=|\{c+d(\bmod p)\mid c\in A,d\in B\}|=|A|$，那么就有 $A'=A+B$。于是对于任意的

$e \in A,$ 存在唯一 $f \in A,$ 使 $e+a=f+b,$ 即 $e=f+(b-a)$ 由于 A 选取的任意性，这意味着 b-a=0（mod p）于是与 B 为二元组矛盾！ Q.E.D

利用该引理，我们给出**第二种证明**：

不妨令 $0 \le \mathrm{a}_1 \le \mathrm{a}_2 \le \cdots \le \mathrm{a}_{2p-1} \le p-1$ 为模 p 后的非降序排序序列

若 $\exists a_i = a_{i+p-1}$，那么有 $\mathrm{a}_i + \mathrm{a}_{i+1} + \cdots + \mathrm{a}_{i+p-1} \equiv 0 (\mathrm{mod}\ p)$ 定理成立

现假设 $\forall i, a_i \ne a_{i+p-1}$，构建如下集合：

$$A_1 = \{a_1, a_p\}, A_2 = \{a_2, a_{p+!}\}, ..., A_{p-1} = \{a_{p-1}, a_{2p-2}\}, A_p = \{a_{2p-1}\}$$

由 C-D 定理，$|A_1 + A_2| \ge 3, |(A_1 + A_2) + A_3| \ge 4, \cdots$，$|A_1 + A_2 + ... + A_{p\text{-}1}| \ge p$

于是（$A_1 + A_2 + ... + A_{p\text{-}1}$)=$\mathbb{Z}_{\mathrm{p}}$ 从而 $\mathrm{a}_1, \mathrm{a}_2, \cdots, \mathrm{a}_{2p-2}$ 中一定有 n-1 个数的和与 a_{2p-1} 模 p 同余，即这 n-1 个数加上 a_{2p-1} 的和被 p 整除。 Q.E.D

对于 Erdös-Ginzburg-Ziv 定理的几何意义，可以看作至少需要多少个在数轴上的整点，才能挑出 p 个整点，使这些点的重心坐落在数轴的整点上。

将情况扩展至二维平面，得到**结论**：从任意 4p−3 个二维平面的整点 $\mathrm{a}_1, \mathrm{a}_2, \cdots, \mathrm{a}_{4p-3}$ 中必能选出 p 个整点 $\mathrm{a}_{i1}, \mathrm{a}_{i2}, \cdots, \mathrm{a}_{ip}$，其中 i1<i2<…<ip，满足这些点的重心是整点，即 $p \mid \sum_{k=1}^{p} x_{ik}$ 且 $p \mid \sum_{k=1}^{p} \mathrm{y}_{ik}$，其中 x_k, y_k 表示点 a_k 的横、纵坐标。感兴趣的同学可自行研究。