

1 四平方和定理

1.1 背景介绍

四平方和定理说明每个正整数均可表示为 4 个整数的平方和。它是费马多边形数定理和华林问题的特例。1743 年，瑞士数学家欧拉发现了一个著名的恒等式： $(a^2 + b^2 + c^2 + d^2)(x^2 + y^2 + z^2 + w^2) = (ax + by + cz + dw)^2 + (ay - bx + cw - dz)^2 + (az - bw - cx + dy)^2 + (aw + bz - cy - dx)^2$ 根据上述欧拉恒等式可知如果正整数 m 和 n 能表示为 4 个整数的平方和，则其乘积 mn 也能表示为 4 个整数的平方和。1751 年，欧拉又得到了另一个一般的结果。即对任意奇素数 p ，同余方程 $x^2 + y^2 + 1 \equiv 0 \pmod{p}$ 必有一组整数解 x, y 满足 $0 \leq x < \frac{p}{2}$, $0 \leq y < \frac{p}{2}$

至此，证明四平方和定理所需的全部引理已经全部证明完毕。此后，拉格朗日和欧拉分别在 1770 年和 1773 年作出最后的证明。

1.2 定理叙述

定理 1. 设 $n \in \mathbb{N}^+$ ，则存在 $a, b, c, d \in \mathbb{N}$ 使得 $n = a^2 + b^2 + c^2 + d^2$ 。

1.3 证明概述

只需证明所有素数可以写为四平方和。 $2 = 1^2 + 1^2 + 0^2 + 0^2$ ，因此只需证明奇质数可以表示成四个整数的平方和。

证明. 根据欧拉 1973 年的结果，存在 $0 < x, y < \frac{p}{2}$ 使得 $x^2 + y^2 + 1^2 + 0^2 = kp$ 。令 $m_0 := \min\{k \in \mathbb{N}^+ : \exists x_i, i = 1, 2, 3, 4, kp = \sum_{i=1}^4 x_i^2\}$ 。从 $0 < x, y < \frac{p}{2}$ 可知 $m_0 < p$ 。

若 m_0 是偶数，且 $m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2$ 。不失一般性设 x_1, x_2 的奇偶性相同，奇偶分析知 x_3, x_4 的奇偶性也相同，则 $x_1 + x_2, x_1 - x_2, x_3 + x_4, x_3 - x_4$ 均为偶数。从而 $\frac{m_0}{2} p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$ 但 $\frac{m_0}{2} < m_0$ ，与 m_0 的定义矛盾。

现在用反证法证明 $m_0 = 1$ 。设 $m_0 > 1$ 。易知 m_0 不可整除 x_1, x_2, x_3, x_4 的最大公因数，否则 m_0^2 可整除 $m_0 p$ ，则得 m_0 是 p 的因数，但 $1 < m_0 < p$ 且 p 为质数，矛盾。故存在不全为零、绝对值小于 $\frac{1}{2}m_0$ （注意 m_0 是奇数在此的重要性）的整数 y_1, y_2, y_3, y_4 使得

$$y_i \equiv x_i \pmod{m_0}, 0 < \sum_{i=1}^4 y_i^2 < 4\left(\frac{1}{2}m_0\right)^2 = m_0^2, \sum_{i=1}^4 y_i^2 \equiv \sum_{i=1}^4 x_i^2 \equiv 0 \pmod{m_0}$$

从而 $\sum_{i=1}^4 y_i^2 = m_0 m_1$ ，其中 $m_1 \in \mathbb{N}^+, m_1 < m_0$ 。下证 $m_1 p$ 可以表示成四平方和。令：

$$\begin{cases} z_1 = x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4, z_2 = x_1 y_2 - x_2 y_1 + x_3 y_4 - x_4 y_3 \\ z_3 = x_1 y_3 - x_2 y_4 - x_3 y_1 + x_4 y_2, z_4 = x_1 y_4 + x_2 y_3 - x_3 y_2 - x_4 y_1 \end{cases}$$

则有 $\sum_{i=1}^4 z_i^2 = \sum_{i=1}^4 y_i^2 \times \sum_{i=1}^4 x_i^2$ 。且易知 $z_1 \equiv \sum_{i=1}^4 x_i^2 \equiv 0 \pmod{m_0}$ 。又有 $z_2 \equiv x_1 x_2 - x_2 x_1 + x_3 x_4 - x_4 x_3 \equiv 0 \pmod{m_0}$ ，同理 $z_3, z_4 \equiv 0 \pmod{m_0}$ 。故 z_1, z_2, z_3, z_4 是 m_0 的倍数，令 $z_i = m_0 t_i, i = 1, 2, 3, 4$ ，则有 $m_0^2 \sum_{i=1}^4 t_i^2 = m_0 m_1 m_0 p$ ，从而 $\sum_{i=1}^4 t_i^2 = m_1 p < m_0 p$ ，与 m_0 的定义矛盾。□