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。

历史

- 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或四元数的概念可知如果正整数 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。于是为证明原命题只需证明每个素数可以表示成 4 个整数的平方和即可。

- 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 $0 \leq x < \frac{p}{2}$，$0 \leq y < \frac{p}{2}$ (引理一)

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。

证明

根据上面的四平方和恒等式及算术基本定理，可知只需证明质数可以表示成四个整数的平方和即可。

$2=1^2+1^2$，因此只需证明奇质数可以表示成四个整数的平方和。

根据引理一，奇质数 p 必有正倍数可以表示成四个整数的平方和。在这些倍数中，必存在一个最小的。设该数为 m_0p。又从引理一可知 $m_0 < p$。

证明 m_0 不会是偶数

设 m_0 是偶数，且 $m_0p = x_1^2 + x_2^2 + x_3^2 + x_4^2$。由奇偶性可得知必有两个数或四个数的奇偶性相同。不失一般性设 x_1, x_2 的奇偶性相同，x_3, x_4 的奇偶性相同，$x_1 + x_2, x_1 - x_2, x_3 + x_4, x_3 - x_4$ 均为偶数，可得出公式：

$\frac{m_0p}{2} = \left(\frac{x_1+x_2}{2}\right)^2 + \left(\frac{x_1-x_2}{2}\right)^2 + \left(\frac{x_3+x_4}{2}\right)^2 + \left(\frac{x_3-x_4}{2}\right)^2$

$\frac{m_0}{2} < m_0$，与 m_0 是最小的正整数使得的假设 m_0p 可以表示成四个整数的平方和不符。

证明 $m_0 = 1$

现在用反证法证明 $m_0 = 1$。设 $m_0 > 1$。

- m_0 不可整除 x_i 的最大公因数，否则 m_0^2 可整除 m_0p，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）整数的 y_1, y_2, y_3, y_4 使得 $y_i = x_i \pmod{m_0}$。

$$\begin{aligned} 0 < \sum y_i^2 &< 4(\tfrac{1}{2}m_0)^2 = m_0^2 \\ \sum y_i^2 &\equiv \sum x_i^2 \equiv 0 \pmod{m_0} \end{aligned}$$

可得 $\sum y_i^2 = m_0m_1$，其中 m_1 是正整数且小于 m_0。

- 下面证明 m_1p 可以表示成四个整数的平方和，从而推翻假设。

令 $\sum z_i^2 = \sum y_i^2 \times \sum x_i^2$，根据四平方和恒等式可知 z_i 是 m_0 的倍数，令 $z_i = m_0t_i$，

$$\begin{aligned} \sum z_i^2 &= \sum y_i^2 \times \sum x_i^2 \\ m_0^2 \sum t_i^2 &= m_0m_1m_0p \\ \sum t_i^2 &= m_1p < m_0p \end{aligned}$$

矛盾。

引理一的证明

将和为 $p-1$ 的剩余两个一组的分开, 可得出 $\frac{p+1}{2}$ 组, 分别为 $(0,p-1),(1,p-2),...,(\frac{p-1}{2},\frac{p-1}{2})$。将模 p 的二次剩余有 $\frac{p+1}{2}$ 个，分别为 $0,1^2,2^2,...,(\frac{p-1}{2})^2$。

若 $\frac{p-1}{2}$ 是模 p 的二次剩余，选取 $x<\frac{p}{2}$ 使得 $x^2\equiv\frac{p-1}{2}$，则 $1+x^2+x^2\equiv 0 \pmod p$，定理得证。

若 $\frac{p-1}{2}$ 不属于模 p 的二次剩余，则剩下 $\frac{p-1}{2}$ 组，分别为 $(0,p-1),(1,p-2),...,(\frac{p-3}{2},\frac{p+1}{2})$，而模 p 的二次剩余仍有 $\frac{p+1}{2}$ 个，由于 $\frac{p+1}{2}>\frac{p-1}{2}$ ，根据抽屉原理，存在 $1+x^2+y^2\equiv 0 \pmod p$。

Category: 加性数论 Category: 包含证明的条目 Category: 数论中的平方 Category: 数论定理