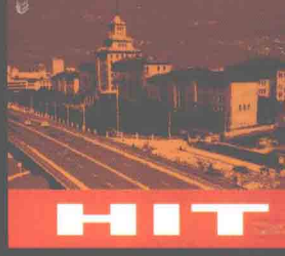

数论经典著作系

Quadratic Sum

平方和

冯克勤 著

哈尔滨工业大学出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

Quadratic Sum
平方和

冯克勤 著

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

内容简介

全书共分四章及附录:第一章整数平方和——能表示吗?第二章再谈整数平方和——有多少种表示法?第三章-1是平方和吗?第四章多项式平方和。本书适合于高等院校师生及相关专业研究人员、数学奥林匹克竞赛选手和教练员以及数学爱好者。

图书在版编目(CIP)数据

平方和/冯克勤著. —哈尔滨:哈尔滨工业大学出版社,2011.3

ISBN 978-7-5603-3219-2

Ⅰ.①平… Ⅱ.①冯… Ⅲ.①平方和 Ⅳ.①O156.1

中国版本图书馆CIP数据核字(2011)第038422号

策划编辑 刘培杰 张永芹
责任编辑 李广鑫
出版发行 哈尔滨工业大学出版社
社 址 哈尔滨市南岗区复华四道街10号 邮编150006
传 真 0451-86414749
网 址 http://hitpress.hit.edu.cn
印 刷 哈尔滨市石桥印务有限公司
开 本 787mm×1092mm 1/16 印张7 字数130千字
版 次 2011年3月第1版 2011年3月第1次印刷
书 号 ISBN 978-7-5603-3219-2
定 价 18.00元

前言

在解决一个数学问题时，如果我们没有获得成功，原因常常在于我们没有认识到更一般的观点，从这种观点看来，眼下要解决的问题不过是一连串有关问题中的一个环节. 采用这样的观点之后，不仅我们所研究的问题会容易得到解决，同时还会获得一种能应用于有关问题的普遍方法……

希尔伯特：《数学问题》，1900 年在巴黎第二届国际数学家大会上的演讲

本书中要讲的问题是：平方和.

正整数是否都可写成两个整数的平方和？通过简单的试验便可知道，例如从 1 到 30 这 30 个正整数中，3，6，7，11，12，14，15，19，21，22，23，24，27，28 和 30 这 15 个数不能表成两个整数的平方和，而其余 15 个整数是可以的（例如 $1=1^2+0^2$，$2=1^2+1^2$，$4=2^2+0^2$，$5=2^2+1^2$，等等）. 那么，究竟什么样的正整数可以表成两个整数的平方和？

正整数是否都可写成三个整数的平方和？仍然作简单的试验便可知道，在不能表成两个整数平方和的上面那 15 个数当中，除了 7，15，23 和 28 之外，其余 11 个数均可表成三个整数的平方和（例如 $3=1^2+1^2+1^2$，$6=1^2+1^2+2^2$，$11=1^2+1^2+3^2$，等等），而 7，15，23 和 28 均不是三个整数的平方和. 那么，究竟什么样的正整数可以表成三个整数的平方和？

7,15,23 和 28 不能表成三个整数的平方和,但是都可以表成四个整数的平方和:$7=1^2+1^2+1^2+2^2$,$15=1^2+1^2+2^2+3^2$,$23=1^2+2^2+3^2+3^2$,$28=1^2+1^2+1^2+5^2$. 换句话说,30 以内的正整数均可表成四个整数的平方和. 如果你愿意试验一下更大的正整数,便会发现它们似乎都可以. 那么,是否每个正整数均可表成四个整数的平方和呢?

更进一步,一个正整数 n 有多少种不同的方法可表成二个(三个或四个……)整数的平方和? 例如 $25=(\pm5)^2+0^2=0^2+(\pm5)^2=(\pm3)^2+(\pm4)^2=(\pm4)^2+(\pm3)^2$ 共有 12 种方法表成二整数平方和. 将 n 表成两个(三个或四个……)整数平方和的表法数有没有简单的计算公式?

-1(以及所有负整数)显然不能表成整数的平方和,-1 也不能表成有理数或者实数的平方和. 但是在复数域中,-1 显然是平方和:$-1=0^2+i^2$,因 $i^2=-1$. 那么,给了任意一个域 F,如何判别 -1 是否为域 F 中元素的平方和? 如果 -1 是域 F 中元素的平方和,那么 -1 至少是域 F 中几个元素的平方和? 如果 -1 不是 F 中元素的平方和,那么域 F 中什么样的元素才是 F 中元素的平方和?

一个实系数多项式 $f(x_1,x_2,\cdots,x_n)$ 是否可表成一些实系数多项式的平方和? 如果 $f(x_1,x_2,\cdots,x_n)$ 可如此表示,即 $f(x_1,x_2,\cdots,x_n)=g_1(x_1,x_2,\cdots,x_n)^2+g_2(x_1,x_2,\cdots,x_n)^2+\cdots+g_m(x_1,x_2,\cdots,x_n)^2$,其中 $g_1,g_2,\cdots,g_m$ 均是实系数多项式,那么对于任意实数 $a_1,a_2,\cdots,a_n$,$f(a_1,a_2,\cdots,a_n)=g_1(a_1,a_2,\cdots,a_n)^2+g_2(a_1,a_2,\cdots,a_n)^2+\cdots+g_m(a_1,a_2,\cdots,a_n)^2\geqslant0$. 对于任意实数都取非负值的多项式叫做正定的. 那么,反过来,正定的实系数多项式是否一定可表成一些实系数多项式的平方和? 如果不能,那么它是否可表成一些实系数有理函数的平方和? ……

这些关于"平方和"的数学问题听起来通俗易懂,但其实都是很不简单的,每个问题的背后都有精彩的数学典故. 首先,这些问题都是由著名数学家进行研究并得到解决的. 关于正整数表成二整数平方和问题,早在公元前丢番图就作过研究. 费马于 1642 年在给梅森(Mersenne)的信中就已基本上猜出了正确的结论,欧拉也研究过这个问题. 但是第一个完全解决二整数平方和与三整数平方和问题的是德国大数学家高斯(1801 年,24 岁). 而四整数平方和问题则是由法国数学家拉普拉斯解决的(1772 年,23 岁). 他证明了:每个正整数均可表成四整数平方和. 关于 -1 在域 F 中是否为平方和这个问题,德国数学家阿廷(E. Artin)和施莱尔(Schreier)于 1926 年进行了深刻的研究. 而 -1 在域 F 中表成平方和所需最少元素个数,德国数学家费斯特(Pfister)于 1967 年给出十分漂亮的结果. 关于正定实系数多项式是否可表成实系数多项式平方和,是由德国大数学家希尔伯特于 1888 年进行研究,答案在多数情形均是否定的. 这促使他退一步问:正定实系数多项式是否一定可表成实系数有理函数的平方和? 这

是他于1900年巴黎第二届国际数学家大会上所提的23个著名数学问题中的第17个问题.这问题于1927年由阿廷所解决.本书将介绍这几段很不简单的数学史.

其次,上述数学家在研究和解决各种平方和问题的时候,提出和创造了新的数学思想和方法.这些新的数学思想和方法对于推动数学发展所起的作用和巨大意义,甚至超过了解决某些具体数学问题本身的价值.正如我们在前言一开头引用的希尔伯特那段话所指出的,这些数学家以高观点来考察平方和问题,把它作为更一般问题的一个环节,创造了研究和解决更广泛问题的普遍方法,甚至由此产生出一些富有生命力的新的数学分支.高斯研究二整数平方和问题的方法,经过库默尔和希尔伯特等人的发展,形成了数论一个新的分支——代数数论.爱森斯坦等人对于整数平方和表法个数公式的研究,产生了椭圆模函数理论和模形式理论.阿廷和施莱尔对于-1是否为平方和的研究,建立了形式实域理论.正是利用这个理论,一年后阿廷解决了希尔伯特第17个问题.费斯特对-1表成平方和所需最少元素个数等问题的研究,建立了新的二次型代数理论……通过各种平方和问题,本书也想向大家介绍这些数学家创造了哪些新的数学思想和方法,如何推动数学的发展,并由此建立了哪些新的数学分支.

最后,我们所以能够为中学师生写这本小册子,是因为关于平方和的数学问题、数学结果,甚至相当一部分数学证明都是非常初等的.我们所选取的材料就所需知识面来讲均属于初等数学范围.除了中学教材之外,只需要一点初等数论知识.为了读者方便,本书将这些初等数论知识写成一个简单的附录,放在书后供大家参考.如果说大家有什么困难,可能会是数学修养方面的问题.而本书的主要目的正是想通过平方和问题使大家开阔眼界.我们试图通过对平方和这些初等数学材料讲述非初等的数学思想.把这些材料当做通向了解高等数学思想方法的媒介和桥梁,以提高中学师生的数学修养,了解近代数学的一些侧面和轮廓.除此之外,我们也希望大家从中领略到一点数学美.

冯克勤

一九八九年二月于合肥

目录

整数平方和 —— 能表示吗?

第一章

设 k 是一个正整数。本节要解决的问题是:哪些正整数 n 可以表示成 k 个整数的平方和? 以后把"k 个整数的平方和"简称为"k 平方和".

一平方(和)问题是很平凡的. 若 n 为某个整数的平方,则 n 叫做完全平方数. 设

$$n = p_1^{r_1} p_2^{r_2} \cdots p_s^{r_s}$$

是 n 的标准素因子分解式(见附录),则 n 为完全平方数,当且仅当 $r_1, r_2, \cdots, r_s$ 均为偶数,而一般地,每个正整数 n 均可唯一地表示成

$$n = m^2 m'$$

其中 m 为正整数,而 m' 不被任何素数的平方除尽. 也就是说,m' 或者为1,或者是一些彼此不同的素数的乘积. 我们将 m^2 和 m' 分别叫做 n 的平方因子部分和无平方因子部分.

以下从二平方和问题谈起.

1.1 二平方和 —— 高斯定理

正整数 n 是否为二平方和,相当于说不定方程

$$x^2 + y^2 = n$$

是否有整数解(x,y). 这个问题丢番图(前409—前325)就研究过. 例如他发现了下面的恒等式:

$$(a^2+b^2)(c^2+d^2)=(ac\mp bd)^2+(bc\pm ad)^2 \qquad ①$$

大家可以将两边展开直接验证这个恒等式的正确性,也可以像高斯一样利用复数:

$$\text{左边}=|a+bi|^2\cdot|c\pm di|^2=|(a+bi)(c\pm di)|^2=$$
$$|(ac\mp bd)+(bc\pm ad)i|^2=\text{右边}$$

并且由这个恒等式直接得到如下重要结论:

引理 1　若正整数 n 和 m 均是二平方和,则 nm 也是二平方和. 于是(用数学归纳法即可证出)任意有限个二平方和之积仍是二平方和.

从这个引理自然会使我们想到首先需弄清哪些素数是二平和. 因为若所有的素数均是二平方和,那么由引理 1 和正整数的素因子分解特性,便可推出每个正整数均为二平方和了. 但不幸(也许是更为有趣)的是:不是所有的素数均为二平方和. 下面的定理圆满地解决了"素数何时为二平方和"这个问题. 虽然费马(Fermat,1601—1665)等人早就提出这个结论,但是第一个证明被高斯认为是由欧拉(Euler,1707—1783)给出的.

定理 1(欧拉)　素数 p 是二平方和的充分必要条件为 $p=2$ 或 $p\equiv 1 \pmod 4$. (换句话说:素数 p 不为二平方和 $\Leftrightarrow p\equiv 3 \pmod 4$.)

证明　必要性的证明是容易的. 由于 $2=1^2+1^2$,以下设 p 是奇素数. 如果 p 是二平方和,即 $p=x^2+y^2$,其中 x 和 y 是整数. 则 $x^2+y^2\equiv 0 \pmod p$,即 $x^2\equiv -y^2 \pmod p$. 易知 $p\nmid y$,于是同余式两边可同时除以 y^2,得到

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

这意味着 -1 是模 p 的二次剩余,因此 $p\equiv 1 \pmod 4$(见附录). 这就证明了必要性.

充分性的证明就困难多了. 我们要证明当 $p\equiv 1 \pmod 4$ 时,p 是二平方和. 首先,由 $p\equiv 1 \pmod 4$ 知,-1 为模 p 的二次剩余,即有整数 a 使得

$$a^2\equiv -1 \pmod p$$

a 所属模 p 同余类中每个整数均有这个性质,而这个同余类中总有一个整数的绝对值小于 $\frac{p}{2}$(见附录),从而我们不妨假定 $|a|<\frac{p}{2}$. 于是 $p\mid a^2+1$,即 $a^2+1=mp$,其中 m 为正整数,并且 $mp=a^2+1<\left(\frac{p}{2}\right)^2+1<p^2$,从而 $1\leqslant m\leqslant p-1$. 至此,我们证明了一个初步结果:在 $1,2,\cdots,p-1$ 当中存在整数 m,使得 mp 为二平方和.

现在我们以 m_0 表示使得 m_0p 为二平方和的最小正整数. 由上面所证可知

m_0 是存在的，并且 $1 \leqslant m_0 \leqslant p-1$. 我们的目的显然是要证 $m_0 = 1$（从而 p 为二平方和）. 证明用反证法：如果 $m_0 \geqslant 2$，而 $m_0 p = x_1^2 + y_1^2$，其中 x_1 和 y_1 为整数，在 x_1 和 y_1 所属的模 m_0 同余类中总可分别取整数 x_0 和 y_0，使得 $|x_0|$ 和 $|y_0|$ 均不超过 $\frac{m_0}{2}$（为什么可以这样做？），即

$$x_0 \equiv x_1, y_0 \equiv y_1 (\bmod m_0), |x_0|, |y_0| \leqslant \frac{m_0}{2}$$

如果 $x_0 = y_0 = 0$，则导致 $m_0 \mid p$. 但这与 $1 \leqslant m_0 \leqslant p-1$ 矛盾，因此 x_0 和 y_0 不全为零，即

$$0 < x_0^2 + y_0^2 \leqslant \left(\frac{m_0}{2}\right)^2 + \left(\frac{m_0}{2}\right)^2 = \frac{m_0^2}{2}$$

由于

$$x_0^2 + y_0^2 \equiv x_1^2 + y_1^2 = m_0 p \equiv 0 (\bmod m_0)$$

可知 $x_0^2 + y_0^2 = m' m_0$，其中 m' 为整数. 并且由 $0 < x_0^2 + y_0^2 = m' m_0 \leqslant \frac{m_0^2}{2}$ 可知 $1 \leqslant m' \leqslant \frac{m_0}{2} < m_0$. 再由恒等式 ① 得出

$$m' m_0^2 p = (x_0^2 + y_0^2)(x_1^2 + y_1^2) = (x_0 x_1 + y_0 y_1)^2 + (x_0 y_1 - y_0 x_1)^2$$

但是

$$x_0 x_1 + y_0 y_1 \equiv x_1^2 + y_1^2 \equiv 0 (\bmod m_0)$$

$$x_0 y_1 - y_0 x_1 \equiv x_1 y_1 - y_1 x_1 \equiv 0 (\bmod m_0)$$

因此 $A = \frac{1}{m_0}(x_0 x_1 + y_0 y_1)$ 和 $B = \frac{1}{m_0}(x_0 y_1 - y_0 x_1)$ 均是整数，并且

$$A^2 + B^2 = \frac{m' m_0^2 p}{m_0^2} = m' p$$

即 $m'p$ 也是二平方和. 但是 $1 \leqslant m' < m_0$，这便与 m_0 的最小性相矛盾. 唯一的可能性便是 $m_0 = 1$，即 p 为二平方和. 这就完成了定理 1 的证明.

上述证明的后一部分采用的方法是费马首创的，叫做“无穷递降法”. 因为它的证明实质是：如果 $m_0 p$ 为二平方和并且 $m_0 \geqslant 2$，则求出另一正整数 $m_1 (= m') < m_0$，使得 $m_1 p$ 也为二平方和. 如果仍旧 $m_1 \geqslant 2$，则按同样办法又可找到正整数 $m_2 < m_1$，使得 $m_2 p$ 也为二平方和 …… 于是我们得到递降的正整数序列 $m_0 > m_1 > m_2 > \cdots$. 但它们均是正整数，从而不能无穷递降下去，所以必须经过有限步达到值 1. 我们以后在研究四平方和问题时还要用到这个方法.

现在讨论任意正整数 n 何时为二平方和. 下面定理给出完整的答案，结论本身也是于 17 世纪由费马等人猜测出来，但是第一个证明是由高斯（Gauss，1777—1855）于 1801 年给出的.

定理 2(高斯)　正整数 n 是二平方和的充分必要条件为:n 的无平方因子部分 m' 或者为 1,或者 m' 的每个素因子均是二平方和(由定理 1,这意味着 m' 的每个素因子均为 2 或模 4 余 1 的素数).

证明　充分性是容易的:设 $n = m^2m'$,如果 m' 的每个素因子均是二平方和,由引理 1 知 m' 为二平方和,而 $m^2 = m^2 + 0^2$ 为二平方和,从而 $n = m^2m'$ 为二平方和.

现在证明必要性,即若 n 为二平方和,则 n 的无平方因子部分 m' 或者为 1,或者 m' 的每个素因子均是二平方和. 我们对 n 作数学归纳法. 当 $n = 1$ 时命题显然成立. 现设命题对所有小于 n 的正整数均正确,而 n 为二平方和:$n = x^2 + y^2$,我们要证 m' 的所有素因子均为二平方和. 如果 n 的所有素因子均为二平方和,则 m' 的素因子也是如此,从而证毕. 下设 n 有素因子 p 不是二平方和. 由定理 1 知 $p \equiv 3 \pmod 4$,于是 $x^2 + y^2 = n \equiv 0 \pmod p$. 如果 $p \nmid x$,则

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

这在 $p \equiv 3 \pmod 4$ 时是不可能的,因此 $p \mid x$. 同样地 $p \mid y$. 于是 $p^2 \mid x^2 + y^2 = n$,即 $n' = \frac{n}{p^2}$ 是整数,并且由 $n' = \left(\frac{x}{p}\right)^2 + \left(\frac{y}{p}\right)^2$ 知 n' 为二平方和. 由归纳假设知 n' 的无平方因子部分的每个素因子均是二平方和. 但是易知 $n' = \frac{n}{p^2}$ 和 n 具有同样的无平方因子部分 m',这就证明了定理 2.

【例】　1 989 和 1 990 是否为二平方和?

解　$1\,989 = 3^2 \cdot 13 \cdot 17$,无平方因子部分为 $m' = 13 \cdot 17$. 由于 $13 \equiv 17 \equiv 1 \pmod 4$,从而 1 989 是二平方和. 事实上,由于 $13 = 2^2 + 3^2, 17 = 1^2 + 4^2$,于是

$$1\,989 = 3^2 \cdot |2 + 3i|^2 \cdot |1 + 4i|^2 =$$
$$3^2 \cdot |(2 + 3i)(1 + 4i)|^2 = 3^2 \cdot |-10 + 11i|^2 =$$
$$3^2(10^2 + 11^2) = 30^2 + 33^2$$

或者
$$1\,989 = 3^2 \cdot |(2 - 3i)(1 + 4i)|^2 = 3^2 \cdot |14 + 5i|^2 =$$
$$42^2 + 15^2$$

而 $1\,990 = 2 \cdot 5 \cdot 199$,其中 199 为素数并且 $199 \equiv 3 \pmod 4$,由定理 2 知 1 990 不是二平方和.

从上面例子可以看出,一个正整数 n 可能有许多种表成二平方和的方法. 即不定方程 $n = x^2 + y^2$ 可能有许多整数解 (x,y). 如 1 989 就有 16 种方式表示成二平方和 $x^2 + y^2$,其中

$$(x,y) = (\pm 30, \pm 33), (\pm 33, \pm 30),$$
$$(\pm 42, \pm 15), (\pm 15, \pm 42)$$

而本质上则只有两种解:$(x,y) = (30,33)$ 和 $(42,15)$,其他解均可由这两个解

加上负号或交换 x 和 y 的取值而得到. 一般地,正整数 n 共有多少方法表示成二平方和,则是比"能否表成二平方和"更为深入的问题,我们将它留在下章讨论. 但目前可以对 n 为素数的情形解决此问题. 由于 $2=1^2+1^2$ 本质上只有一种表示方法. 以下只需再讨论 p 是模 4 余 1 的素数.

定理3(高斯)　设 p 是素数,并且 $p\equiv 1(\mathrm{mod}\ 4)$,则 p 本质上只有一种方法表成二平方和.

证明　设 $p=a^2+b^2=A^2+B^2$,其中 a,b,A,B 均为整数. 我们只需证明 $a=A$ 或者 $a=B$ 即可. 由于

$$p^2=(a^2+b^2)(A^2+B^2)=(aA\pm bB)^2+(aB\mp bA)^2 \tag{②}$$

$$(aA+bB)(aA-bB)=A^2(a^2+b^2)-b^2(A^2+B^2)=$$
$$A^2p-b^2p\equiv 0(\mathrm{mod}\ p)$$

从而 $p\mid aA+bB$ 或者 $p\mid aA-bB$. 如果 $p\mid aA+bB$,注意 $aA+bB>0$,由式②可知必然 $aA+bB=p$,$aB-bA=0$,于是

$$\frac{a^2}{A^2}=\frac{b^2}{B^2}=\frac{a^2+b^2}{A^2+B^2}=\frac{p}{p}=1$$

因此 $a=A$,$b=B$. 同样若 $p\mid aA-bB$,则由 $aB+bA>0$ 及式②可知 $aB+bA=p$,$aA-bB=0$. 仿上面证明即得 $a=B$,$b=A$. 证毕.

练习　求证:若正整数 n 可表成两个有理数的平方和,则必可表成两个整数的平方和(提示:用定理2).

1.2　四平方和——兼谈域和四元数体

我们在上节圆满解决了二平方和问题. 接下来应当是三平方和问题. 但是四平方和问题有非常漂亮的结果,并且证明与定理2的证明非常相像,所以先讲它. 1770 年,拉格朗日(Lagrange,1736—1813)第一个证明了下面的定理.

定理4(拉格朗日)　每个正整数均是四平方和.

证明　首先请大家验证下面的恒等式:

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)=$$
$$A^2+B^2+C^2+D^2 \tag{③}$$

其中

$$\begin{cases} A=x_1y_1+x_2y_2+x_3y_3+x_4y_4 \\ B=x_1y_2-x_2y_1-x_3y_4+x_4y_3 \\ C=x_1y_3+x_2y_4-x_3y_1-x_4y_2 \\ D=x_1y_4-x_2y_3+x_3y_2-x_4y_1 \end{cases} \tag{④}$$

由恒等式③可知,有限多个四平方和的乘积仍旧为四平方和. 因此我们只需证每个素数 p 均为四平方和即可. 由于 $2 = 1^2 + 1^2 + 0^2 + 0^2$,以下设 p 为奇素数. 考虑集合

$$M = \left\{x^2 \mid x = 0,1,2,\cdots,\frac{p-1}{2}\right\}$$

$$N = \left\{-(1 + y^2) \mid y = 0,1,2,\cdots,\frac{p-1}{2}\right\}$$

集合 M 中 $\frac{p+1}{2}$ 个数模 p 彼此不同余. 因若 $x_1^2 \equiv x_2^2 (\mathrm{mod}\ p)$,$0 \leqslant x_1 < x_2 \leqslant \frac{p-1}{2}$,则 $p \mid (x_1 + x_2)(x_2 - x_1)$. 但是

$$1 \leqslant x_2 \pm x_1 \leqslant \frac{p-1}{2} + \frac{p-1}{2} = p - 1$$

这就导出矛盾. 同样地,集合 N 中 $\frac{p+1}{2}$ 个数模 p 也彼此不同余. 但是 M 和 N 元素个数合在一起为 $\frac{p+1}{2} + \frac{p+1}{2} = p + 1$,而模 p 同余类只有 p 个. 从而集合 M 中必有某个 x^2 和集合 N 中某个 $-(1 + y^2)$ 是模 p 同余的. 即存在整数 x 和 y 使得 $0 \leqslant x, y \leqslant \frac{p-1}{2}$,并且 $x^2 \equiv -(1 + y^2)(\mathrm{mod}\ p)$,即

$$x^2 + y^2 + 1 \equiv 0(\mathrm{mod}\ p)$$

于是有正整数 m,使得

$$mp = x^2 + y^2 + 1 = x^2 + y^2 + 1^2 + 0^2$$

并且由

$$x^2 + y^2 + 1 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 < p^2$$

可知 $1 \leqslant m \leqslant p - 1$. 换句话说,我们证明了:存在整数 m,$1 \leqslant m \leqslant p - 1$,使得 mp 为四平方和.

接下来又和定理 2 的证明一样,用无穷递降法. 以 m_0 表示使得 $m_0 p$ 为四平方和的最小正整数. 由上面所证知这样的 m_0 是存在的,并且 $1 \leqslant m_0 \leqslant p - 1$. 我们的目的是证明 $m_0 = 1$. 若不然,即若 $m_0 \geqslant 2$,设 $m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2$,其中 x_1,x_2,x_3,x_4 均为整数. 如果 m_0 是偶数,则

$$x_1 + x_2 + x_3 + x_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p \equiv 0(\mathrm{mod}\ 2)$$

在 x_1,x_2,x_3,x_4 中至少有两个数同时为偶或同时为奇. 不妨设它们为 x_1 和 x_2,则 $x_1 \equiv x_2(\mathrm{mod}\ 2)$. 再由上面同余式即知 $x_3 \equiv x_4(\mathrm{mod}\ 2)$. 于是 $\frac{1}{2}(x_1 \pm x_2)$ 和 $\frac{1}{2}(x_3 \pm x_4)$ 均是整数,并且

$$\frac{m_0}{2}p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$$

即$\frac{m_0}{2}p$为四平方和. 这与m_0的最小性相矛盾,所以m_0必为奇数. 这时,存在整数y_i,使得

$$y_i \equiv x_i (\bmod m_0), |y_i| < \frac{m_0}{2}, i = 1,2,3,4$$

如果$y_i (1 \leqslant i \leqslant 4)$均为0,则$m_0 | x_i (1 \leqslant i \leqslant 4)$. 从而$m_0^2 | x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p$,于是$m_0 | p$,这与$2 \leqslant m_0 \leqslant p - 1$相矛盾. 因此$y_i (1 \leqslant i \leqslant 4)$不全为零,即

$$1 \leqslant y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4 \cdot \left(\frac{m_0}{2}\right)^2 = m_0^2$$

又由于

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p \equiv 0 (\bmod m_0)$$

于是$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m' m_0$,其中$m'$为整数,并且

$$1 \leqslant m' m_0 < m_0^2, \text{即} 1 \leqslant m' < m_0$$

现在利用恒等式③:

$$m' m_0^2 p = (x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = (A^2 + B^2 + C^2 + D^2)$$

其中A,B,C,D的表达式如式④所示. 我们有

$$A = x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0 p \equiv 0 (\bmod m_0)$$

$$B = x_1 y_2 - x_2 y_1 - x_3 y_4 + x_4 y_3 \equiv x_1 x_2 - x_2 x_1 - x_3 x_4 + x_4 x_3 \equiv 0 (\bmod m_0)$$

同样地有$C \equiv D \equiv 0 (\bmod m_0)$,从而

$$m' p = \left(\frac{A}{m_0}\right)^2 + \left(\frac{B}{m_0}\right)^2 + \left(\frac{C}{m_0}\right)^2 + \left(\frac{D}{m_0}\right)^2$$

是将$m'p$表成四个整数平方和. 但是$1 \leqslant m' < m_0$,这与m_0的最小性相矛盾. 因此必然有$m_0 = 1$,即p为四平方和. 这就完成了定理4的证明.

拉格朗日定理是这样漂亮,以至于我们对它本身已没有话要说,只好再说些题外的话. 首先,由于7不是三平方和,从而使每个正整数均为k平方和的最小k值是4. 其次,进一步要问:每个正整数n表成四平方和共有多少种方法?这也留到下节研究. 最后,让我们回过头来看一下恒等式③. 这个恒等式的直

接验证并不难,初中学生都应当会做. 问题是这个恒等式是怎样发现的? 因为科学的本质在于发现新事物,而验证是第二位的. 这个问题有历史上的兴趣,我们也想结合这个数学典故给大家谈谈"域"这个概念.

高斯利用复数 $i^2=-1$ 证明了关于二平方和的恒等式①. 高斯的观点是:将求不定方程 $n=x^2+y^2$ 的整数解这个纯属整数范围内的问题,放到复数集合上来考察,即写成 $n=|x+iy|^2$. 而恒等式①的证明不过利用了关于复数绝对值的一个简单事实:任意二复数的绝对值之积等于它们之积的绝对值,即 $|\alpha||\beta|=|\alpha\beta|$. 我们是否能找到一个别的什么"数"的集合代替复数集合,然后用这种新的数集合的性质证明恒等式③?

复数集合中是可以进行加减乘除四则运算的(其中作除法时除数不为0),并且加法和乘法满足结合律、交换律和分配律. 这样的代数结构在近世代数中叫做域. 今后把复数域记作 **C**. 事实上,**C** 有许多子集合也是域,如有理数域 **Q**、实数域 **R** 等. 再比如,设整数 d 不是完全平方数,则 $\sqrt{d}$ 不是有理数. 令

$$Q(\sqrt{d})=\{\alpha+\beta\sqrt{d}\mid \alpha,\beta\in\mathbf{Q}\}$$

这是比有理数域 **Q** 更大的域. 请大家验证集合 $\mathbf{Q}(\sqrt{d})$ 满足域的上述所有条件. 这里我们只举例验证 $\mathbf{Q}(\sqrt{d})$ 中可作除法:设 $\alpha+\beta\sqrt{d}$ 和 $\gamma+\delta\sqrt{d}$ 均属于 $\mathbf{Q}(\sqrt{d})$,其中 $\alpha,\beta,\gamma,\delta\in\mathbf{Q}$,并且 $\gamma+\delta\sqrt{d}\neq 0$. 因此 γ 和 δ 不全为0. 由 d 不是完全平方数可知

$$(\gamma+\delta\sqrt{d})(\gamma-\delta\sqrt{d})=\gamma^2-\delta^2 d\neq 0$$

因此

$$\frac{\alpha+\beta\sqrt{d}}{\gamma+\delta\sqrt{d}}=\frac{(\alpha+\beta\sqrt{d})(\gamma-\delta\sqrt{d})}{\gamma^2-d\delta^2}=\frac{\alpha\gamma-\beta\delta d}{\gamma^2-d\delta^2}+\frac{\beta\gamma-\alpha\delta}{\gamma^2-d\delta^2}\sqrt{d}$$

而 $\frac{\alpha\gamma-\beta\delta d}{\gamma^2-d\delta^2}$ 和 $\frac{\beta\gamma-\alpha\delta}{\gamma^2-d\delta^2}$ 均是有理数,即 $\frac{\alpha+\beta\sqrt{d}}{\gamma+\delta\sqrt{d}}$ 属于 $\mathbf{Q}(\sqrt{d})$,从而 $\mathbf{Q}(\sqrt{d})$ 中可作除法.

我们前面所谈的域都是比复数域 **C** 小的域,那么是否有比 **C** 更大的域呢? 设 x 是一个未定元(事实上,只要 x 不是任何复系数多项式的根即可). 设 $f(x)$ 和 $g(x)$ 是两个复系数的(关于 x 的)多项式,并且 $g(x)$ 不恒等于0,则 $\frac{f(x)}{g(x)}$ 叫做有理函数. 所有这种有理函数对于大家所学过的通常加减乘除运算形成一个域,这叫做复数域 **C** 上的有理函数域,表示成 $\mathbf{C}(x)$. 由于每个非零复数看成是零次多项式,从而 $\mathbf{C}(x)$ 包含 **C**,即 $\mathbf{C}(x)$ 是比 **C** 更大的域. 类似地我们有实数域 **R** 上的有理函数域 $\mathbf{R}(x)$(即多项式系数均是实数),有理数域 **Q** 上的有理函

数域 $\mathbf{Q}(x)$ 等.

另一方面,是否有一种代数结构,它满足域的几乎所有性质,只是乘法不必满足交换律,即 ab 和 ba 不一定相等. 这样的代数结构叫做体. 第一个这样的例子是由哈密尔顿(Hamilton,1805—1865)发现的,叫做四元数体,表示成 H. 它的每个元素(叫做四元数)写成形成

$$\alpha = x_1 + x_2\mathrm{i} + x_3\mathrm{j} + x_4\mathrm{k}$$

其中 x_1, x_2, x_3, x_4 均是实数.

四元数的加减法采取通常形式,即

$$(x_1 + x_1\mathrm{i} + x_2\mathrm{j} + x_3\mathrm{k}) \pm (y_1 + y_2\mathrm{i} + y_3\mathrm{j} + y_4\mathrm{k}) =$$
$$(x_1 \pm y_1) + (x_2 \pm y_2)\mathrm{i} + (x_3 \pm y_3)\mathrm{j} + (x_4 \pm y_4)\mathrm{k}$$

而乘法则有以下的乘法表:

$$\mathrm{ij} = \mathrm{k} = -\mathrm{ji}, \mathrm{jk} = \mathrm{i} = -\mathrm{kj}, \mathrm{ki} = \mathrm{j} = -\mathrm{ik}$$
$$\mathrm{i}^2 = \mathrm{j}^2 = \mathrm{k}^2 = -1$$

并且对每个实数 a 和每个四元数 α, $a\alpha = \alpha a$. 然后用分配律就可作任意两个四元数的乘积. 例如设 x_1, x_2, x_3, x_4 均为实数,则

$$\begin{aligned}&(x_1 + x_2\mathrm{i} + x_3\mathrm{j} + x_4\mathrm{k})(x_1 - x_2\mathrm{i} - x_3\mathrm{j} - x_4\mathrm{k}) =\\ &x_1^2 - x_2^2\mathrm{i}^2 - x_3^2\mathrm{j}^2 - x_4^2\mathrm{k}^2 + (x_2x_1 - x_1x_2)\mathrm{i} +\\ &(x_3x_1 - x_1x_3)\mathrm{j} + (x_4x_1 - x_1x_4)\mathrm{k} -\\ &x_2x_3(\mathrm{ij} + \mathrm{ji}) - x_3x_4(\mathrm{jk} + \mathrm{kj}) - x_4x_2(\mathrm{ki} + \mathrm{ik}) =\\ &x_1^2 + x_2^2 + x_3^2 + x_4^2 \qquad ⑤\end{aligned}$$

我们把 $x_1 - x_2\mathrm{i} - x_3\mathrm{j} - x_4\mathrm{k}$ 叫做四元数 $\alpha = x_1 + x_2\mathrm{i} + x_3\mathrm{j} + x_4\mathrm{k}$ 的共轭,表示成 $\bar{\alpha}$. 而把实数 $(x_1^2 + x_2^2 + x_3^2 + x_4^2)^{\frac{1}{2}}$ 叫做 α 的绝对值,表示成 $|\alpha|$,那么公式⑤表明

$$\alpha\bar{\alpha} = \bar{\alpha}\alpha = |\alpha|^2$$

如果 $\alpha \neq 0$(即 x_1, x_2, x_3, x_4 不全为0),则 $|\alpha| > 0$,从而

$$\alpha \cdot \frac{\bar{\alpha}}{|\alpha|^2} = \frac{\bar{\alpha}}{|\alpha|^2} \cdot \alpha = 1$$

这表明 $\dfrac{\bar{\alpha}}{|\alpha|^2} = \dfrac{1}{x_1^2 + x_2^2 + x_3^2 + x_4^2}(x_1 - x_2\mathrm{i} - x_3\mathrm{j} - x_4\mathrm{k})$ 为 α 的乘法逆元素. 于是对任意两个四元数 α 和 $\beta(\beta \neq 0)$,则四元数 $\dfrac{1}{|\beta|^2}\alpha\bar{\beta}$ 和 $\dfrac{1}{|\beta|^2}\bar{\beta}\alpha$ 分别是方程 $\alpha = x\beta$ 和 $\alpha = \beta x$ 的解. 这就表明四元数集合中有除法运算,不过由于乘法没有交换律(例如 $\mathrm{ij} = -\mathrm{ji}$!),方程 $\alpha = x\beta$ 和 $\alpha = \beta x$ 的解可能不同,所以我们不能将解写成 $\dfrac{\alpha}{\beta}$ 这种分式的形式,于是 H 是体.