有趣的数论名题

YOUQU DE SHULUN MINGTI

周从尧 余未 编著

以数论领域几个非常有名的问题为纲，汇集了计算数论、计算技术，GIMPS计划的最新成果，综合历史人物趣闻、逸事、研究进展过程，通古今、揽中外、共雅俗。本书提供了不少程序，供有兴趣的人士参考，这些程序都是作者编制并通过了上机验证的。只要您对数论有兴趣，且想在现有数论基础上有所突破，都会从本书中得到启发。

哈尔滨工业大学出版社

有趣的数论名题

周从尧　余　未　编著

湖南大学出版社

内 容 简 介

本书以数论领域几个非常有名的问题为纲，汇集了计算数论、计算技术，GIMPS 计划的最新成果，综合历史人物趣闻、逸事、研究进展过程，通古今、揽中外、共雅俗。

本书通俗易懂，加上了本书作者研读的不少心得，以讲故事、拉家常的方式一一呈现给大家，相信会被广泛读者所接受，希望读者群中未来能出现一些新星。

本书提供了不少程序，供有兴趣的人士参考，这些程序都是作者编制并通过了上机验证的。

本书的读者群十分广泛，包括优秀的初高中学生、各种数学培训班学员、大学生、研究生等。只要您对数论有兴趣，且想在现有数论基础上有所突破，都会从本书中得到启发。

图书在版编目(CIP)数据

有趣的数论名题/周从尧，余未编著．

—长沙：湖南大学出版社，2012.6

ISBN 978-7-5667-0201-2

Ⅰ.①有… Ⅱ.①周…②余… Ⅲ.①数论—普及读物

Ⅳ.①0156-49

中国版本图书馆 CIP 数据核字(2012)第 131740 号

有趣的数论名题

Youqu de Shulun Mingti

作　　者：周从尧　余　未　编著

责任编辑：卢　宇　黄　旺　　**责任校对**：祝世英

出版发行：湖南大学出版社　　**责任印制**：陈　燕

社　　址：湖南·长沙·岳麓山　　**邮　　编**：410082

电　　话：0731－88822559(发行部)，88821315(编辑室)，88821006(出版部)

传　　真：0731－88649312(发行部)，88822264(总编室)

电子邮箱：pressluy@hnu.edu.cn

网　　址：http://www.hnupress.com

印　　装：衡阳顺地印务有限公司

开本：787×1092　16 开　　**印张**：10　　**字数**：232 千

版次：2012 年 6 月第 1 版　　**印次**：2012 年 6 月第 1 次印刷

书号：ISBN 978-7-5667-0201-2/0·85

定价：25.00 元

作者简介

周从尧，男，湖南大学退休教授，1944 年出生于江苏盐城，1970 年毕业于清华大学数力系计算数学专业，1970 到 1972 在解放军 0646 部队西湖农场进行劳动锻炼，1972 年到 1973 年在长沙市一中教授数学，1973 年进入湖南省计算技术研究所和湖南大学工作，直到 2002 年退休。曾获获全国科学大会奖 1 项、国家科技进步奖 1 项、湖南省科技进步奖 6 项，发表论文 10 余篇，并获国务院政府津贴，被评为湖南省优秀专家。

余未，女，1974 年生于浙江宁波，1992～1996 年在浙江大学（合并前的杭州大学）数学与信息科学系就读本科，获理学学士学位，1996～1999 年在浙江大学数学系概率论与数理统计专业就读研究生，获理学硕士学位，1999 年至今在宁波大学理学院数学系任教。曾荣获宁波大学 2003 年“课堂教学优秀奖”二等奖，宁波大学 2007 年“课堂教学优秀奖”一等奖，2007～2008 年度浙江省高校第五届青年教师教学技能比赛优秀奖，宁波大学 2010 年“教坛新秀”称号，第四届浙江省高等学校教坛新秀奖。

序

摆在我们面前的这本数学通俗读物，内容丰富，引人入胜。本书的大部分内容与数论有关。数论是一门通古今，贯中西，融雅俗的大学问。为什么这么说呢？数论是最古老的数学分支之一，在当代依然保持着旺盛的青春活力；中国数学家从古至今都在数论的探索与发展中占有一席之地；比较而言，不少著名的数论命题都能为大众所理解（当然，其深入研究另当别论）。

本书的作者之一周从尧是我的大学同窗。当我们还是大一新生时，周从尧就表现出优秀的数学才能，对数学的浓厚兴趣及钻研精神。虽然作者后来并未以数学为自己的专业，但对数学的浓厚兴趣依然保持至今。本书包含着作者对数学之美的欣赏和领悟，在书中不时还可以看到作者自己的心得体会和成果。我想，大部分读者都有这样的共识，就是看数学书，无论是教科书、专著还是小册子，都要眼到、手到、心到。唯有如此，才能真有收获。比如说看这本书的正十七边形那一章，不妨沿着作者的思路，把改进的作图法动手做一遍。游览数学大观园，既要俯身体察细节之美，又要抬头纵览全局之美。作者在费尔马大定理那一章提到了朗兰兹纲领。朗兰兹纲领是继希尔伯特第二问题之后最具雄心的数学现代化纲领，对于广大读者而言，如果能看到大师级的数学家就数学现代化问题写出一本通俗读物，就是莫大的幸事了。

数学教育有三个层次：传授知识，提高能力，培养兴趣。当然，这三者是相互关联，相互交融的。对于大部分人来说，学过的知识可能忘了，能力上也不一定有多少过人之处，但若能始终保持一份对数学的兴趣和热爱，就是一种最可宝贵的文化修养。这对保持和发展我们民族的文化自信、文化自觉是必不可少的。

黄连生

2012 年 3 月于清华园

前　言

数学中有名的问题很多，要同时具备两个特点：有名而有趣，才能引起大家的兴趣，我们精选了 9 个有名而有趣的数论问题，对每一个问题都由浅入深地进行讨论，希望能给读者以指引。

华林问题是数论中的著名问题之一，由爱德华·华林于 1770 年提出来，这个问题是这样的：对于每个正整数，皆存在正整数 $g(k)$，使得每个正整数都可以表示为 $g(k)$ 个自然数的 k 次方之和。其中拉格朗日四平方和问题是华林问题的最简单情况，而拉格朗日四平方和定理是费尔马问题的前哨，又是华林问题的起点，是华林问题中解决得最彻底的问题，我们觉得也很不错，本书作者提供了一个最好理解的证明，并附有例题说明，可加深读者的理解。

高斯的正十七边形，有传奇的故事，高斯本人在数学上有许多辉煌的成就，光专著就有十几本，为什么非要把正十七边形刻在墓碑上，可见正十七边形在他心中的分量。就是这个正十七边形，把几何作图，代数方程，费尔马数巧妙地连在一起，给人们许多美的享受。

高次代数方程的求解是一个困扰了数学家几个世纪的问题，直到一批天才的出现，这种情况才得以改观，这其中最著名的要数伽罗华，这位只活了 21 年的数学家在数论领域做出了不可磨灭的贡献。自古以来的二十五位大数学家，伽罗华就是其中之一。

梅森素数，数海中的明珠，虽然到目前只有 47 个，它在与其他素数的竞赛中总是夺得最大素数的冠军，验证的方法又美妙无比。同时它又与完美数共同进退，有一个梅森素数，就有一个完美数，如果 2^p-1 是梅森素数，则 $2^{p-1}(2^p-1)$ 就是完美数，这中间还有中国人周海中的猜想，及本书作者的反猜想。

我们大家都知道哥德巴赫猜想，其实费尔马问题名声一点不比哥德巴赫小，甚至还大一些，但其中 $n=3$，$n=4$ 的证明，具有初中水平的人还是可以看得懂的，所以入选，而且还有一个原因，就是此问题 1995 年已经被英国数学家怀尔斯彻底解决了。

费尔马数 $F_n=2^{2^n}+1$，成千上万的人曾经为它奋斗过，在现在和将来可以预计的年代内，必定还有更多的人会为他奋斗，任重而道远，所以搜集到本书以供欣赏和研究，比如说吧，$F_{33}=2^{2^{33}}$ 究竟是合数还是素数，现在的计算机这么强大，这个问题居然没有得到解决。关于这个问题，我们查阅了最新资料，列表供读者参考，同时还做了 F_8，F_9 等费尔马数的验证。我们估计，费尔马数的解决远比费尔马大定理还难。

谢尔宾斯基数是指使得所有形如 $k*2^n+1$ 的数均为合数的奇整数 k，比如 78 557 $*$ 2^n+1 永远是合数，所以 78 557 是谢尔宾斯基数。其实谢尔宾斯基数问题是这样的，对

$k*2^n+1$ 这样形式的数，还有比 78 557 小的 k，也保证 $k*2^n+1$ 这样形式的数永远是合数吗？历史上杰斯基曾经宣布：1～383 的奇数肯定没有这样的 k，383～78 557 之间他找到 91 个这样的 K，即谢尔宾斯基数。可是计算机验证后，这 91 个数全部被否定，比如 $N=3\ 061*2^n+1$，在 $n=33\ 288$ 时居然是素数，这个数的确不小，验证它是素数的确不轻松，当时算错，是有可能的。

$3x+1$ 问题，又称克拉茨问题，角古问题，表面很好玩，实则深不可测，有人建议作为下一个费尔马问题，自然不同凡响，应该选上。我们还编写了程序，计算了不少函数，供读者欣赏和研究。

黎曼猜想问题，虽然描述有些困难，但由于它的重要性，完美性，和它居然是 1000 个命题的基础，所以我们还是要尽量用浅显易懂的方式将它描述清楚，并提供三个程序及图形数据，供读者理解。

为了方便读者的理解和今后工作学习中可能的需求，我们配备了不少程序，这些程序都是通过上机验证的，还为读者准备了一个可以计算 1 亿以内的所有素数的程序，只要运行它，就可以生成您所需要的结果，供读者学习与参考。天上繁星颗颗，数海明珠就像天上的繁星，正等着大家去发现；地上麦浪滚滚，就待有志者来收获。

由于作者水平有限，时间仓促，缺点和错误难免，请大家批评和指正。

编　者

2011 年 12 月

目　次

1 华林问题简介

1.1 引 言

华林问题是数论中的著名问题之一. 1770 年,爱德华·华林(E. Waring,1734～1798)提出一个猜想:对于每个正整数,皆存在正整数 $g(k)$,使得每个正整数都可以表示为 $g(k)$个自然数的 k 次方之和. 例如,$2=1^2+1^2$,是 2 个自然数的平方和;$33=2^4+2^4+1^4$,是 3 个自然数的四次方和;$79=2^4+2^4+2^4+2^4+1^4+1^4+1^4+1^4+1^4+1^4+1^4+1^4+1^4+1^4+1^4+1^4+1^4+1^4+1^4$,是 19 个自然数的四次方和.

1909 年,大卫·希尔伯特首先用比较复杂的方法证明了 $g(k)$的存在性. 1943 年,U. V. 林尼克给出了关于 $g(k)$存在性的另一个证明. 然而,尽管 $g(k)$的存在性已被证明,但人们仍无法知晓 $g(k)$与 k 之间的关系. 华林自己推测 $g(2)=4$,$g(3)=9$,$g(4)=19$. 1770 年,拉格朗日证明了四平方和定理,指出 $g(2)=4$;1909 年亚瑟·韦伊费列治证明了 $g(3)=9$;1859 年,柳维尔证明了 $g(4)\leqslant 53$;1978 年陈景润得到了 $g(4)\leqslant 27$ 的证明;本书著者在 1982 得到了 $g(4)\leqslant 23$ 的证明.

哈代和李特尔伍德得到 $g(4)\leqslant 21$,1986 年巴拉苏布拉玛尼安证明 $g(4)=19$. 1896 年马力特得到 $g(5)\leqslant 192$;1909 年韦伊费列治将结果改进为 $g(5)\leqslant 59$;1964 年陈景润证明了 $g(5)=37$.

本章就 $k=2$ 时,任何一个自然数均为不超过 4 个自然数的平方和,提供一个最好理解的证明. $g(2)$问题又被称作拉格朗日四平方和定理.

1.2 定理及其证明

引理 1 $(a^2+b^2+c^2+d^2)(x^2+y^2+z^2+w^2)=(ax+by+cz+dw)^2+(ay-bx+cw-dz)^2+(az-bw-cx+dy)^2+(aw+bz-cy-dx)^2$.

读者只要展开即可验证.

引理 2 对任意奇素数 p,同余方程 $x^2+y^2+1\equiv 0 \pmod p$ 必存在 $0\leqslant x,y\leqslant (p-1)/2$的 x,y 满足该同余方程.

证明 (Ⅰ)令 $m=0,1,\cdots,(p-1)/2$,则 $m^2=0,1,4,9,\cdots,(p-1)^2/4$,对模 p 不同余(共$\frac{p+1}{2}$个元素).

以 $p=17$ 为例,共 9 个项(0,1,4,9,16,25,36,49,64)对模 17 不同余,即共 9 个项(0,

1,4,9,16,8,2,15,13)对模 17 不同余.

下面用反证法证明之.假设该序列中第 i 项、第 j 项同余,也就是第 i 项为 $i^2=a\times p+r$,(其中 r 为余数,$0\leqslant i\leqslant(p-1)/2$),第 j 项为 $j^2=b\times p+r$(其中 r 为余数,$0\leqslant j\leqslant(p-1)/2$),两式相减得 $(i+j)(i-j)=(a-b)\times p$,因为 $|i+j|+|i-j|\leqslant p-1$,p 为素数,此式不可能成立.

(Ⅱ)令 $m=0,1,2,\cdots,(p-1)/2$,则 $-m^2-1=-1,-2,-5,-10,\cdots,-(p-1)^2/4-1$ 对模 p 也不同余(共 $\frac{p+1}{2}$ 个元素).

以 $p=17$ 为例,共 9 个项(−1,−2,−5,−10,−17,−9,−37,−50,−65)对模 17 不同余,即共 9 个项(16,15,12,7,0,8,14,1,3)对模 17 不同余.

(Ⅲ)结合(Ⅰ)(Ⅱ),情况就不同了,(Ⅰ)(Ⅱ)两组,各自对模 p 不同余,但两组合为一组,由于序列中共有 $p+1$ 个元素,而对模 p 来讲,最多只有 0,1,...,$p-1$ 共计 p 个同余类,因此(Ⅰ)中至少存在一个 i 与(Ⅱ)中的一个 j 所对应的元素同余.不妨设 i 对应的是 $x=up+r$,j 对应的是 $-y^2-1=vp+r$,两式相减得 $x^2+y^2+1=(u-v)p$,即 $x^2+y^2+1\equiv 0(\mathrm{mod}p)$.

所以引理 2 得证.

引理 3 对任意奇素数 p,一定存在 k,使得 $x^2+y^2+1^2=kp$,其中 $0\leqslant x,y\leqslant(p-1)/2$.

在引理 2 的证明过程中,我们已经知道 $k=u-v$,尽管我们没有去具体计算 u,v,其实引理 3 是引理 2 的弱化形式,我们只是添加了一个 0.其中的 $k<p$,这是因为 $kp=x^2+y^2+1<(p-1)^2/4+(p-1)^2/4+1<p^2$,所以 $k<p$.

定理 1 任何一个自然数均可表示为不超过 4 个自然数的平方和.

证明 由引理 1,及任何自然数可表示为素数的乘积,易知只要证明任何素数可表示为四个自然数的平方和,则上述定理即可得证.

由引理 3,令 $k=u-v$ 得 $a_1^2+a_2^2+a_3^2+a_4^2=kp$.

(Ⅰ)如果 $k=1$,则定理已经得证,即对任何素数 p 都是四个数的平方和.

(Ⅱ)如果 k 是偶数,$a_1^2+a_2^2+a_3^2+a_4^2=kp$(偶数),$a_1,a_2,a_3,a_4$ 或全奇,或全偶,或两奇两偶,不妨设 a_1,a_2 同奇偶,a_3,a_4 同奇偶,则由 $a_1^2+a_2^2+a_3^2+a_4^2=kp$ 可知

$$\left(\frac{a_1+a_2}{2}\right)^2+\left(\frac{a_1-a_2}{2}\right)^2+\left(\frac{a_3+a_4}{2}\right)^2+\left(\frac{a_3-a_4}{2}\right)^2=(k/2)p \qquad ①$$

即可通过两边除以 2 的方法,不断降低 k 的值.

(Ⅲ)我们只需考虑 k 为奇数的情况.

在 $(-k/2,k/2)$ 的范围展开 a_1,a_2,a_3,a_4 如下:

$$a_i=n_i\times k+\delta_i \qquad ②$$

由引理 1 得

$$(a_1^2+a_2^2+a_3^2+a_4^2)(\delta_1^2+\delta_2^2+\delta_3^2+\delta_4^2)=(a_1\delta_1+a_2\delta_2+a_3\delta_3+a_4\delta_4)^2+(a_1\delta_2-a_2\delta_1+a_3\delta_4-a_4\delta_3)^2+(a_1\delta_3-a_2\delta_4-a_3\delta_1+a_4\delta_2)^2+(a_1\delta_4+a_2\delta_3-a_3\delta_2-a_4\delta_1)^2 \qquad ③$$

将②式代入③式左边第一项得

$$kp=a_1^2+a_2^2+a_3^2+a_4^2$$

$$=(n_1\times k+\delta_1)^2+(n_2\times k+\delta_2)^2+(n_3\times k+\delta_3)^2+(n_4\times k+\delta_4)^2$$
$$=k^2\times(n_1^2+n_2^2+n_3^2+n_4^2)+2k(n_1\times\delta_1+n_2\times\delta_2+n_3\times\delta_3+n_4\times\delta_4)$$
$$+(\delta_1^2+\delta_2^2+\delta_3^2+\delta_4^2) \qquad ④$$

注意④式左边能被 k 整除，而右边前两项也能被 k 整除，所以最后一项 $(\delta_1^2+\delta_2^2+\delta_3^2+\delta_4^2)$ 一定也能被 k 整除. 不妨假设

$$(\delta_1^2+\delta_2^2+\delta_3^2+\delta_4^2)=nk \qquad ⑤$$

又 $nk=(\delta_1^2+\delta_2^2+\delta_3^2+\delta_4^2)<4\,(k/2)^2<k^2$，所以 $n<k$.

再把 $a_i=n_i\times k+\delta_i$ 代入③式右边的后三项，则④式的右边

$$=[a_1\delta_1+a_2\delta_2+a_3\delta_3+a_4\delta_4]^2+k^2[(n_1-n_2)+(n_3-n_4)]^2$$
$$+k^2[(n_1-n_3)-(n_2-n_4)]^2+k^2[(n_1-n_4)+(n_2-n_3)]^2$$

而③式的左边 $=kp\times nk$ 带 k^2 因子，所以两边一定可以约去公共因子 k^2，最后得：

$$np=[a_1\delta_1+a_2\delta_2+a_3\delta_3+a_4\delta_4]^2/k^2+[(n_1-n_2)+(n_3-n_4)]^2$$
$$+[(n_1-n_3)-(n_2-n_4)]^2+[(n_1-n_4)+(n_2-n_3)]^2 \qquad ⑥$$

其中 $n<k$，使得 kp 前的系数 k 又降低到 n.

经过(Ⅱ)(Ⅲ)两步，kp 中的 k 会不断地降下去，最终会降到 1，达到(Ⅰ)的要求.

综合(Ⅰ)(Ⅱ)(Ⅲ)及任何自然数可表示为素数的乘积，可证明一切自然数均可表示为不超过 4 个自然数的平方之和.

例如：$13^2+1^2+4^2+0^2=6\times31$.

其中 $k=6$ 为偶数，则 $a_1+a_2=14$，$a_1-a_2=12$，$a_3+a_4=4$，$a_3-a_4=4$，$k/2=3$，利用①式可以得到 $7^2+6^2+2^2+2^2=3\times31$，由②式得 $7=2\times3+1$，$6=2\times3+0$，$2=1\times3-1$，$2=1\times3-1$. 再利用③式得

$$(a_1^2+a_2^2+a_3^2+a_4^2)(\delta_1^2+\delta_2^2+\delta_3^2+\delta_4^2)$$
$$=(7^2+6^2+2^2+2^2)[1^2+0^2+(-1)^2+(-1)^2]$$
$$=[7+0+(-2)+(-2)]^2+[0-6+(-2)-(-2)]^2$$
$$+[-7-(-6)-2+0]^2+[-7+(-6)-0-2]^2$$
$$=3^2+6^2+3^2+15^2$$

两边同除以 3^2 得 $1^2+2^2+1^2+5^2=1\times31$.

1.3 华林问题简介

上一节详细介绍的拉格朗日四平方和问题是华林问题的最简单情况，现在再简单介绍华林问题的另外几个结论. 结论不是目前最好的，目前的最好结论都需要高深的工具，回忆前人用简单工具得到的结论是很有趣的.

1770 年，爱德华·华林提出华林猜想，对于每个正整数，皆存在正整数 $g(k)$，使得每个正整数都可以表示为 $g(k)$ 个自然数的 k 次方之和，这是华林小 $g(k)$ 问题.

若将“对于每个正整数”改为“充分大的自然数”，则是华林大 $G(k)$ 问题，大 G 问题的进展比较缓慢，到目前连 $G(3)$ 都还没有完全解决.

定理 2 任何一个正整数均可表示为 50 个整数的四次方之和(即 $g(4)\leqslant 50$).

证明 利用恒等式:

$$\begin{aligned}6(a^2+b^2+c^2+d^2)^2 &= (a+b)^4+(a-b)^4+(c+d)^4+(c-d)^4\\ &\quad +(a+c)^4+(a-c)^4+(b+d)^4+(b-d)^4\\ &\quad +(a+d)^4+(a-d)^4+(b+c)^4+(b-c)^4 \qquad ⑦\end{aligned}$$

(1)当 $n\geqslant 81$ 时,$n=6N+r$,这里 $r=0,1,2,81,16,17$(r 依次由 $n\equiv 0,1,2,3,4,5 \pmod 6$)来决定).

首先根据上一节,N 为四个数的平方,即 $n=6(u^2+v^2+s^2+t^2)+r$,而对于每一个 $6u^2,6v^2,6s^2,6t^2$,又因为 $u(v,s,t)$可表示 e,f,g,h 四个整数的平方和,而得到 $6u^2=6(e^2+f^2+g^2+h^2)^2$.

由恒等式⑦得

$6u^2=6(e^2+f^2+g^2+h^2)^2=12$ 个数的四次方之和,所以 $6(u^2+v^2+s^2+t^2)$可表示为 48 个四次方之和,最后 $r=0,1,2,81,16,17$ 为最多 2 个数的四次方之和.

(2)$n<81$ 时,最多 19 个数的 4 次方之和.

总之任一个自然数可以表示为 50 个自然数的四次方之和.

注意:Liouville 在 1859 年证明了 $g(4)\leqslant 53$,1909 年 Wieferich 用初等方法证明了 $g(4)\leqslant 37$,1933 年,Dickson 用同样的方法改进为 $g(4)\leqslant 35$,中间还经过陈景润的 27,在陈景润的 27 之后,本书作者也曾独立证明了 $g(4)\leqslant 23$. 1986 年巴拉苏布拉玛尼安证明了 $g(4)=19$.

定理 3 对于充分大的正整数,$g(3)\leqslant 13$.

用 C_s 来表示一个可以用 s 个非负立方数之和来表示的数.

设 z 取遍 $6k+1$ 的数,对每一个区间 I_z,其下界为 $\Phi(z)=11z^9+(z^3+1)^3+125^3$,其上界为 $\Psi(z)=14z^9$. 当 z 较大时,区间 I_{z+1} 与区间 I_z 有重叠,这是因为 $\Phi(z+6)<\Psi(z)$,因此保证每一个自然数 n 的值必在某一个区间,而不会漏掉,并满足:

$$11z^9+(z^3+1)^3+125^3\leqslant n\leqslant 14z^9$$

每一个自然数 n 可表示为

$$n=N+8*z^9+6*m*z^3 \qquad ⑧$$

(下面有证明)

其中

$$N=C_5,0<m<z^6 \qquad ⑨$$

又根据四平方和定理

$$m=x_1^2+x_2^2+x_3^2+x_4^2 \qquad \text{其中 } 0<x_i<m*z^3$$

所以

$$\begin{aligned}n &= N+8z^9+6*z^3(x_1^2+x_2^2+x_3^2+x_4^2)\\ &= N+\sum_{i=1}^{4}[(z^3+x_1)^3+(z^3-x_1)^3]\\ &= C_5+C_8=C_{13}\end{aligned}$$

(即任意自然数 n 可表示为 13 个自然数的 3 次方之和)

关键只要证明⑧式，关于⑧式的证明如下.

定义 r,s 以及 N 为：

$n\equiv 6r(\mathrm{mod}\ z^3)$ $(1\leqslant r\leqslant z^3)$ （注：对任意 n，用区间套必可找到 z^3）

$n\equiv s+4(\mathrm{mod}\ 6)$ $(0\leqslant s\leqslant 5)$ （从 z^3 出发，立即得 r,s）

$$N=(r+1)^3+(r-1)^3+2(z^3-r)^3+(s*z)^3 \qquad ⑩$$

这样 $N=C_5$，而且

$$0<N<(z^3+1)^3+3z^9+125z^3=\Phi(z)-8*z^9\leqslant n-8*z^9 \qquad ⑪$$

所以

$$8*z^9<n-N<14*z^9 \qquad ⑫$$

对⑩式用模 z^3，则

$$N\equiv(r+1)^3+(r-1)^3-2r^3=6r\equiv n\equiv n-8z^9 \quad (\mathrm{mod}\ z^3) \qquad ⑫$$

对任意 x 有 $x^3\equiv x(\mathrm{mod}\ 6)$ 及 $z=6k+1$

再对⑩式用模 6，得

$$N\equiv r+1+r-1+2(z^3-r)+sz=2z^3+sz$$

$$\equiv 2z+sz\equiv(2+s)*z\equiv 2+s\equiv n-2\equiv n-8\equiv n-8z^9 \quad (\mathrm{mod}6) \qquad ⑬$$

从而 $n-N-8z^9$ 是 $6z^3$ 的倍数，设为 m 倍，这就是⑧式.

定理得证.

定理 4 $g(3)\leqslant 13$.

上个定理中，当 $z\geqslant 373$ 时，区间重叠，$g(4)\leqslant 13$ 成立，相当于 10^{25}，那么对于小于 373 的数怎么办呢？好在 $1\leqslant n\leqslant 240$，$n=C_8$，$1\leqslant n\leqslant 40\ 000$ 已经验证，均为 C_8，而 40 000 到 10^{25}，只要连续 5 次速降（或爬山），就可从 10^{25} 速降到 40 000 了，所谓速降即从 $n=240+N_0=240+10^{25}$ 中减去一个尽可能大的数 $m_0=[N_0^{1/3}]$，则

$$0\leqslant N_0\leqslant 10^{25},N_1=N_0-m_0^3\leqslant 3N_0^{2/3}(N_0^{1/3}-m_0)<3N_0^{2/3}$$

则有

$$N_0=N_1+m_0^3,m_0=[N_0^{1/3}],0\leqslant N_1<3N_0^{2/3}$$

$$N_1=N_2+m_1^3,m_1=[N_1^{1/3}],0\leqslant N_2<3N_1^{2/3}$$

$$\cdots\cdots$$

$$N_4=N_5+m_4^3,m_4=[N_4^{1/3}],0\leqslant N_5<3N_4^{2/3}$$

最后，

$$n=240+N_0=240+N_5+m_0^3+m_1^3+m_2^3+m_3^3+m_4^3$$

$$N_5<3N_4^{2/3}<3(3*N_3^{2/3})^{2/3}<\cdots<27(10^{25}/27)^{(2/3)^5}<35\ 240<40\ 000$$

$240+N=C_8$，n 是 C_{13}.

注意：$g(3)$ 的最好结果为 $g(3)=9$，猜想为 $G(3)=5$，此问题还没有解决.

以上是华林问题的 2 次、3 次、4 次的情况，更高幂次的有如下结果.

定理 5 $g(k)$ 的下界：$g(k)\geqslant 2^k+[(3/2)^k]-2$.

这个定理非常好，如：$g(2)=4$，$g(3)=9$，$g(4)=19$，$g(5)=37$，…，$k<471\ 600\ 000$ 均正确.

定理 6 $G(k)$的下界：$G(k)\geqslant k+1$.

本定理给出了最好的统一的下界，如 $g(3)\geqslant 4$.

定理 7 $G(4)$的下界：$G(4)\geqslant 16$.

因为 $x^4\equiv 0,1(\mathrm{mod}\ 16)$，所以 $16m+15$ 形式的数至少是 15 个数的四次方之和. 所以 $G(4)\geqslant 15$，已经比上一结果 $G(k)\geqslant k+1$ 好得多了，再进一步 31 是 16 个数的 4 次方之和，所以 $G(4)\geqslant 16$.

定理 8 $G(k)$有如下的下界：

(1)如果 $k=2^m$，或 $k=3*2^m$，则 $G(k)=2^{m+2}$；

(2)如果 $k=p^m(p-1)$，且 $p>2$，则 $G(k)=p^{m+1}$；

(3)如果 $k=p^m(p-1)/2$，且 $p>2$，则 $G(k)=(p^{m+1}-1)/2$；

(4)其他 $G(k)\geqslant k+1$.

应用 $G(6)$时，由于 $6=3*2=3(3-1)=7-1=(13-1)/2$，分别对应于 8,9,7,6，其中(2)给出了最强的下界 9.

关于 $G(k)$上界的猜想：

(1)对于 $k=2^m$，及 $m\geqslant 2$，$G(k)=4k$；

(2)其他 $G(k)\leqslant 2k+1$.

1.4 相关定理及猜想

(1)两平方和定理：任何 $4n+1$ 形式的素数 p 可以表示为两个数的四次方之和.

(2)三平方和定理：n 非 $4^k(8m+7)$的数可用三个数的四次方之和来表示.

(3)四平方和定理：对任意自然数，定理不能再改进了，因为 $8m+7$ 形式的数不能用少于 4 个数的四次方之和表示. 比如 $7=2^2+1+1+1$，$15=3^2+2^2+1+1$.

(4)九立方和定理：任何自然数为九个自然数的立方和.

(5)16 四次方和定理：任何自然数为 16 个自然数的四次方和.

(6)37 五次方和定理：任何自然数为 37 个自然数的五次方和.

(7)73 六次方和定理：任何自然数为 73 个自然数的六次方和.

(8)Euler 猜想：任何自然数为 $2^k+\left(\frac{3}{2}\right)^k-2$ 个自然数的 k 次方和. 此为莱昂哈德·欧拉之子 J. A. 欧拉猜想，至 1990 年，对于 $6<k<471\ 600\ 000$，此式已经被计算机验证为正确.

2 永垂不朽的正十七边形

2.1 引 言

二千多年前，古希腊数学家曾深入研究如何利用尺规作内接正多边形的问题. 在《几何原本》一书中，欧几里德已经知道用尺规作出圆内接正三边形、正四边形、正五边形，甚至正十五边形.

然而，似乎更容易完成的正七、九、十一……边形却未能做出. 欧几里德之后的 2 000 多年中，有关正多边形作图，未能向前迈进一步.

因此，我们可以想象得到，当 1796 年，年仅 19 岁的高斯宣布他发现了正十七边形的作图方法时，会在数学界引起多么巨大的轰动.

高斯完成正十七边形的工作，源于老师的一个不经意的失误. 原来老师每天都给高斯开小灶，晚上做一个难题，就相当于当今的因材施教，或者奥数培训吧，某一天老师又给高斯出了一道难题. 第二天，晚上熬了一夜的高斯不好意思地对老师说，辜负了您的期望，花了一个夜晚才把题目做出来. 老师接过高斯的手稿，看完后大吃一惊，真是不可想象，一个 2 000 多年来未解决的难题，居然被十九岁的高斯一个晚上解决了！设想一下，如果老师当时仔细一点，就不会将这个题目给高斯，而高斯如果知道这是个 2 000 多年未解决的世界难题，一定就有畏难情绪，很可能一时也解决不了. 这真是应了中国的两句话，老师是“无心插柳柳成荫”，高斯是“初生牛犊不怕虎”.

在经过继续研究后，高斯最终在 1801 年对整个问题给出了一个漂亮的解答. 高斯指出，如果仅用圆规和直尺，作圆内接正 n 边形，当 n 满足如下特征之一方可做出：

①$n=2^m$；(m 为正整数)

②边数 n 为素数且形如 $n=2^{2^m}+1(m=0,1,2\ldots)$，即费尔马素数；(费尔马素数见第 6 章)

③边数 $n=2^m * p_1 * p_2 * p_3 \ldots * p_k$，其中 p_1、p_2、$p_3 \cdots p_k$ 为互不相同的费尔马素数.

由高斯的结论，具有素数 p 条边的正多边形可用尺规作图的必要条件是 p 为费尔马素数. 由于我们现在得到的费尔马素数只有前五个费尔马素数，那么可用尺规作图完成的正素数边形就只有 3、5、17、257、65537.

进一步，可以做出的有奇数条边的正多边形也就只能通过这五个数组合而得到. 这样的组合数只有 31 种. 而边数为偶数的可尺规做出的正多边形，边数或是 2 的任意次正整数幂或与这 31 个数相结合而得到.

就这样，正多边形作图问题、费尔马数问题、方程的二次根式解问题，几个表面上并不