The Collection of Difficult Problem of Elementary Number Theory

(The Second Volume)

初等数论难题集

（第二卷）

上

主　编　刘培杰

副主编　周晓东　田廷彦　许逸飞

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

The Collection of Difficult Problem of Elementary Number Theory

(The Second Volume)

初等数论难题集

（第二卷）

上

主　编　刘培杰

副主编　周晓东　田廷彦　许逸飞

哈爾濱工業大學出版社

HARBIN INSTITUTE OF TECHNOLOGY PRESS

内 容 简 介

本书共分7章:第1章同余,第2章数列中的数论问题,第3章多项式,第4章数论与函数,第5章二次剩余与同余方程,第6章不定方程,第7章数论与组合.

本书适合于数学奥林匹克竞赛选手和教练员,高等院校相关专业研究人员及数论爱好者.

图书在版编目(CIP)数据

初等数论难题集.第2卷.上/刘培杰主编.—哈尔滨:哈尔滨工业大学出版社,2010.12

ISBN 978-7-5603-2921-5

Ⅰ.①初… Ⅱ.①刘… Ⅲ.①初等数论-解题 Ⅳ.①0156.1-44

中国版本图书馆CIP数据核字(2010)第223124号

策划编辑 刘培杰
责任编辑 张永芹
封面设计 孙茵艾
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34 字数662千字
版 次 2011年2月第1版 2011年2月第1次印刷
书 号 ISBN 978-7-5603-2921-5
印 数 1~3000册
定 价 128.00元(上、下册)

◎前言

在初等数学和数学竞赛中，几何、代数、数论、组合都是“超级大户”.几何需要不少基本知识，而组合杂题（不算计数和组合恒等式，以下所谓的组合都指组合杂题）则是出了名的“支离破碎”，它们处于数学竞赛的两极；数论则介乎两者之间.尽管它们都需要高超的、令人赏心悦目的技巧.

不过，如此一来，倒使数论成为离直觉比较远的了，为什么这样说呢？因为几何问题的构思是“有章可循”的（在与当代平面几何专家叶中豪先生的无数次探讨中，我们深深感觉到这一点），即使再难也不可能解不出，而组合杂题则仅仅依赖于一两个奇怪的想法，像变魔术一样，更依赖于出题者的直觉.但数论题则不然，只要其中一个数字差一点点，就完全可能从一道普通奥数题甚至低幼级问题，变为一道无人能解的世界难题.所以，几何的命题靠的是原有结果的堆砌，简单结果组合出不凡的结论；组合的命题则是从技巧出发，做题的人面临的“风险”是：想到了就是几分钟的事，想不到就是一辈子的事.数论与它们都不太一样（当然也仅仅是相对而言），它不是命题者从定理和技巧出发，而是从某个比较漂亮的结论出发，慢慢地猜出来的；于是数论题无非三种结果：

(1)无人能做出的猜想;

(2)能解决,但无法排除高等工具;

(3)可以成为奥数试题.

做奥数的数论题,如百思不得其解,其实就是没有看出问题本身的实质,变成第(1)或第(2)类问题了.

在高中数学奥林匹克竞赛中,初等数论的最高知识和技巧无非是:模、费马小定理和欧拉定理、二次剩余、中国剩余定理和无穷递降法;最高难度无非是某题掩盖了以上事实作为实质,不容易挖掘出来.也就是说,"暗信息"没有变成"明信息".显然,几何中"暗信息"最多,而组合最少,数论居中.暗信息与直觉、聪明才智不同,是你必须知道的东西.比如说,某些题是绕不过一些暗信息的,如果你没有想到或不知道这些暗信息,那你就不可能把那道题做出来.

在生活中,暗信息大量地存在着.比如出门坐车,身旁的某个陌生人究竟是不是小偷、通缉犯?买东西,质量究竟好不好?我不知道,这跟我的聪明才智有没有关系;而对于癌症这样的大课题来说,人们也无法凭自己的直觉和逻辑推理,很快就找到最好的配方或医疗方式,只好一个个地尝试.在这过程中,聪明才智需要吗?当然需要一点,但是面对复杂异常的实验,小聪明恐怕帮不上什么关键性的大忙.显然,在人类的科学探索中,绝大多数情形是通过实验、经验来挖暗信息,与智商关系不是特别大.数学竞赛处于直觉、聪明和知识、暗信息的交界处,这无疑是世界全部知识体系中极小的一部分,但也已是无穷无尽:我们每次做完一道比较困难的奥数题,总觉得深有体会,似乎"功力"又增长了一点,但是面对下一道难题,又开始一筹莫展了.

因此,奥数难题有两种:一种是真正地依赖于直觉和天才,看过答案之后自然无话可说;另一种则需要某些"暗信息",也就是说我知道需要依赖于某个不太难的结论,但一时不知道是哪个,这在不等式中比较常见,几何亦是如此.有这样一道作图题:已知相交两圆,圆不知,问如何只用直尺画出连心线?这依赖于一些结论:平行弦、弦的中点、中位线,这些都是要做出来的.如果碰巧知道这些(并不困难),此题就迎刃而解,如果碰巧不知道,那就麻烦大了.在数论中,有时也知道做某题要用到同余,但就是不知道该模什么数;再如:设大于1的整数 n 满足每个不同素因子的指数都是2(例如 $2^2\times3^2\times7^2$),证明 n 不整除它的全体因子之和 $\sigma(n)$.如果你知道形如 m^2+m+1 的数无 $3k+2$ 型因子(m,k 均为正整数,可用费马小定理快速证明.再比如,对于大于1的正整数 n,求证 2^n-1 不整除 3^n-1),此题就不很难,否则确有一定难度,你还要"摸索、发现"上述"暗信息".歧路一多,到达目的地就困难许多,而"暗信息"是帮助我们克服歧路的有效工具.上面的这道题,还有许许多多的奥数问题,都有一个共同点:即单单凭借智商似乎很难想得出来,而一个智商不太高但很勤勉、很善于学习的人,能解出来也不是什么稀罕事.要知道数学竞赛题目的难度不可无限升高,最高的也得有最少数的人做得出来,"全军覆没"的题不应该出.怀尔斯证明费马大定理的论文中,一开始就提到40多位当代数学家(包括几位菲尔兹奖得主)的工作,不要说100年,即使是在50

年前,他就是再聪明也休想解决费马大定理.

有人可能认为前一类题目好,其实未必,后一类题目循序渐进,环环相扣,对于积累经验、提升功力、学习进步很有好处.做前一类题,像是徒手爬一座座孤零零的小山,而做后一类题,就是掌握了一定的工具后爬一座大山,尽管走走停停,但最终是"会当凌绝顶,一览众山小".用不了多久,数学功夫就能今非昔比.毕竟我们是在进行数学竞赛,而不是智商竞赛.这一现象在高等数学研究中更为明显.可以想象费马大定理会有一个相对比较初等的证明,但那肯定迂回曲折得多.历史上如有名的素数定理、华林猜想等都是先有高等证明,再有(相对)初等证明的.初等证明的特点是技巧高,缺点是结果不够强.

说了这么多,无非是要告诉大家,没有人具有无穷的天才,所以很多东西是要学的.像费马小定理、欧拉定理,或是微积分中的一些简单公式,都是费马、牛顿、莱布尼茨、欧拉等大师琢磨了上百年的东西,现在看来这些东西似乎都不难,难道这些历史上的大师就这么懒、这么笨吗?千万不要有这个错觉,大师们有很多工作,但历史证明有些不那么重要;能够被历史留下来的,不是最难的结果,而是最重要的结果.对于数学竞赛来说,某个结果用得很频繁,"出镜率"高,就能说明它重要,是一个定理(当然反过来说能称为定理的不一定都很有用).所以,即使是某个定理本身不再是暗信息,它的重要性、它的用法对于一个生手来说也许仍是暗信息!而出题者无非可能在这方面认识多一些,所以他把某个重要定理的应用非常隐蔽地出到某个题目中去,而解题者高不高明,就要看他对那些定理和技巧的领悟的程度了.

科学、数学以及高雅艺术都有这样一个需要学习、需要积累的过程,在此之中我们认为是渐悟、顿悟兼而有之,也就是阶梯式的上进(平的是渐悟,直的是顿悟).现在的一些流行歌曲或快餐文化比较肤浅,只要满足紧张忙碌的人们在一点松懈之余得到消遣就可以了,从它的功能上讲也是尽到了用处,无可厚非.当然,一个人若不满足于此,还想要循序渐进地了解一些比较深入的东西,我们觉得还是应该选择研习科学(特别是数学)或高雅艺术(如古诗、古典音乐),其目的之一就是提高自己的修养.现在一些十分自我的年轻人无意于此,客观上也是因为从繁重的教育和工作中没有得到提高修养的机会;提高修养的唯一途径就是自觉自愿地学习(至少在中学及以后有了这方面意识时),不是为了升学、职称而参加考试的那种学习,那种学习不仅不能提高修养,甚至还会使人对真正意义上的学习产生厌恶之情.爱因斯坦就是被可怕的考试搞得整整一年不想看书,后来他对填鸭式的教育做了相当多的批评.但尽管如此,人们(比如周光召)还是说,爱氏要生长在中国才彻底没戏了.

有人说过,培养对数学的感悟能力,再也没有比初等数论更加合适.历代数学大师对数论赞誉有加.过去也陆续出过一些数论习题的小册子,以及潘承洞、潘承彪编写的很难超越的数论教材.在几何、不等式与分析领域早有类似著作问世.尤其是波利亚、舍贵的《数学分析中的问题和定理》,更是一代名著.我们写这书,主要是为了给读者提供一个学习数论的平台,至少在这一点上,我们的初衷与波利亚、舍贵应该是一致的.

本书中绝大多数题由刘培杰搜集,田廷彦添加了少量问题,主要是参与整理;另有大约

300 题由周晓东提供,其中有约 100 题来自于 Peter Vandendriessche 和 Hojoo Lee 的 Problems in Elementary Number Theory,之前周晓东陆续在 www. mathoe. com 做了翻译、解答. 另外 200 题左右主要来自于平时讲义的积累,大多是国外各类竞赛题及数论资料.

两卷内容大体做如下安排:第 1 卷是初等数论中最基本的内容,即引进同余之前的那部分,包括整除和一些特殊的数的性质(如平方数、素数、进位制等);第 2 卷则主要涉及同余乃至不定方程、数论函数方面的内容. 此次汇编规模甚大,也算是第一次尝试(至少在国内),尽管难免挂一漏万,但希望大家批评指正,待第 2 版时再加以补充和修正.

编著者

2011 年 2 月

◎ 目 录

心得 体会 拓广 疑问

第1章 同 余

1.1 同余基本知识

如无特别,此处字母一般指整数.

设 $m \neq 0$,若 $m \mid a-b$,则 $a \equiv b(\bmod m)$,这两个记号是等价的.

同余具有等价关系,即

(1) $a \equiv a(\bmod m)$;

(2) $a \equiv b(\bmod m) \Leftrightarrow b \equiv a(\bmod m)$;

(3) $a \equiv b(\bmod m), b \equiv c(\bmod m) \Rightarrow a \equiv c(\bmod m)$.

定理 若 $a \equiv b(\bmod m), c \equiv d(\bmod m)$,则

$$a \pm c \equiv b \pm d(\bmod m), ac \equiv bd(\bmod m)$$

由此得推论 $a^n \equiv b^n(\bmod m)$,n 为任意正整数.

平方数、立方数和指数(如 $2^n, 3^n$)在模3、模4、模7、模8等整数模下的取值,十分有用处,这些取值都呈周期性,因此,在模3等意义上取余数,得到的是周期数列.

(4) $ac \equiv bc(\bmod m), c \neq 0$,则

$$a \equiv b\left(\bmod \frac{m}{(c,m)}\right)$$

1.1.1 是否存在 $n \in \mathbf{N}$,使得 $2^{n+1}-1$ 与 $2^{n-1}(2^n-1)$ 都是整数的立方?

(美国纽约,1977年)

解 设有某个 $n \in \mathbf{N}$,使得 $2^{n-1}(2^n-1)$ 是整数的立方. 注意,因为 2^n-1 不被2整除,所以乘积中2的幂指数为 $n-1$. 因此 $n-1=3k$,即 $n=3k+1$,其中 $k \in \mathbf{Z}^*$,但是

$$2^{n+1}-1=2^{3k+2}-1 \equiv 4(7+1)^k-1 \equiv 3(\bmod 7)$$

而任意整数的立方被7除的余数只能是0,1或6,所以

$$(7m)^3 \equiv 0(\bmod 7), (7m \pm 1)^3 \equiv \pm 1(\bmod 7)$$

$$(7m \pm 2)^3 \equiv \pm 1(\bmod 7), (7m \pm 3)^3 \equiv \mp 1(\bmod 7)$$

因此 $2^{n+1}-1$ 不能是整数的立方,于是对任意 $n \in \mathbf{N}$,$2^{n+1}-1$ 与 $2^{n-1}(2^n-1)$ 不能同时是整数的立方.

心得 体会 拓广 疑问

1.1.2 设 $a > 1$ 是自然数,试求所有这样的数,它至少整除一个 $a_n = \sum_{k=0}^{n} a^k, n \in \mathbf{N}$.

(联邦德国,1977 年)

证明 我们证明,所求的集合 M 由所有与数 a 互素的数 $m \in \mathbf{N}$ 组成,如果某个数 $m \in \mathbf{N}$ 与数 a 有公因数 $d > 1$,则 $m \notin M$. 事实上,对任意 $n \in \mathbf{N}$,有

$$(a_n, a) = \left(\sum_{k=0}^{n} a^k, a\right) = \left(1 + a\sum_{k=0}^{n-1} a^k, a\right) = (1, a) = 1$$

因此 a_n 不被 d 整除,从而不被 m 整除. 现在设 $m > 1$,且 $(m, a) = 1$. 由于在 $a_1, a_2, \cdots, a_m, a_{m+1}$ 中可以找出两个数 a_i 与 $a_j, i > j$,它们模 m 同余. 这两个数之差

$$a_i - a_j = \sum_{k=0}^{i} a^k - \sum_{k=0}^{i} a^k = \sum_{k=j+1}^{i} a^k = a^{j+1}\sum_{k=0}^{i-j-1} a^k$$

被 m 整除. 但 a^{j+1} 与 m 互素,因此

$$a_{i-j-1} = \sum_{k=0}^{i-j-1} a^k$$

被 m 整除(因为 $m \neq 1$,所以不可能有 $i - j - 1 = 0$). 因此 $m \in M$. 最后注意 $1 \in M$.

1.1.3 求证:存在无穷多个这样的正整数,它们不能表示成少于十个奇数的平方和.

证明 设正整数 n 能够表示成

$$n = x_1^2 + x_2^2 + \cdots + x_s^2 \qquad ①$$

其中 x_i 为奇数,$i = 1, 2, \cdots, s, 1 \leqslant s \leqslant 9$.

若 $n \equiv 2 \pmod 8$,则由 ① 及 $x_i^2 \equiv 1 \in \pmod 8, i = 1, 2, \cdots, s$ 知 $s \equiv 2 \pmod 8$,即 $s = 2$.

若 $s = 2, 3 \mid n$,则由 ① 及 $x_i^2 \equiv 0, 1 \pmod 3, i = 1, 2$ 知 $x_1 \equiv x_2 \equiv 0 \pmod 3$,从而 $9 \mid n$. 这说明若 $n \equiv 3 \pmod 9$,则 $s \neq 2$.

综上所述,被 8 除余 2,被 9 除余 3,即具有形式 $72k + 66, k = 0, 1, 2, \cdots$ 的正整数便不能表示成 ①,故命题得证.

心得 体会 拓广 疑问

1.1.4 设 $x_1, x_2, \cdots, x_n$ 为 n 个整数，k 为小于 n 的整数，令

$$S_1 = x_1 + x_2 + \cdots + x_k, T_1 = x_{k+1} + x_{k+2} + \cdots + x_n$$

$$S_2 = x_2 + x_3 + \cdots + x_{k+1}, T_2 = x_{k+2} + x_{k+3} + \cdots + x_n + x_1$$

$$S_3 = x_3 + x_4 + \cdots + x_{k+2}, T_3 = x_{k+3} + x_{k+4} + \cdots + x_1 + x_2$$

$$\vdots$$

$$S_n = x_n + x_1 + \cdots + x_{k-1}, T_n = x_k + x_{k+1} + \cdots + x_{n-1}$$

（x_i 循环出现，在 x_n 的后面 x_1 重新出现），又令 $m(a,b)$ 为 i 的个数，使得 S_i 除以3余 a，T_i 除以3余 b，这里 a,b 为0,1或2.

证明：$m(1,2)$ 与 $m(2,1)$ 除以3时余数相同.

（第28届国际数学奥林匹克候选题，1987年）

证明 注意到

$$S_i + T_i = x_1 + x_2 + \cdots + x_n$$

(1) 若 $x_1 + x_2 + \cdots + x_n \not\equiv 0 \pmod 3$，则

$$m(2,1) = m(1,2) = 0$$

(2) 若 $x_1 + x_2 + \cdots + x_n \equiv 0 \pmod 3$，则

$$\sum_{i=1}^{n} S_i = k(x_1 + x_2 + \cdots + x_n) \equiv 0 \pmod 3$$

于是，在 S_i 中，被3除余1的个数与被3除余2的个数之差能被3整除，则

$$3 \mid m(2,1) - m(1,2)$$

即 $m(1,2)$ 与 $m(2,1)$ 被3除时余数相同.

1.1.5 试求 $10^{10} + 10^{10^2} + 10^{10^3} + \cdots + 10^{10^{10}}$ 被7除的余数.

（第5届莫斯科数学奥林匹克，1939年）

解 设 $A = 10^{10} + 10^{10^2} + 10^{10^3} + \cdots + 10^{10^{10}}$.

首先我们证明，若 $6 \mid n - r$，则 $7 \mid 10^n - 10^r (n > r)$. 事实上

$$10^n - 10^r = 10^r(10^{n-r} - 1) = 10^r(10^{6k} - 1) =$$

$$((10^6)^k - 1) \cdot 10^r$$

因为 $10^6 \equiv 1 \pmod 7$，所以

$$(10^6)^k - 1 \equiv 0 \pmod 7$$

即

$$7 \mid 10^n - 10^r$$

另一方面，$6 \mid 10^k - 10 (k \geqslant 1)$，则

$$A - 10 \cdot 10^{10} + 10 \cdot 10^{10} = (10^{10} - 10^{10}) + (10^{10^2} - 10^{10}) + \cdots +$$

$$(10^{10^{10}} - 10^{10}) + 10 \cdot 10^{10}$$

由于 $6 \mid 10^k - 10$，则

心得 体会 拓广 疑问

$$7 \mid 10^{10^k} - 10^{10}$$

于是有

$$A \equiv 10 \cdot 10^{10} (\mathrm{mod}\ 7) = 10^{11} = (7+3)^{11} \equiv 3^{11} \equiv 3^5 \cdot 3^6 (\mathrm{mod}\ 7)$$

由于

$$3^5 \equiv 5 (\mathrm{mod}\ 7)$$

$$3^6 \equiv 1 (\mathrm{mod}\ 7)$$

于是

$$A \equiv 5 (\mathrm{mod}\ 7)$$

即 A 被 7 除的余数是 5.

1.1.6 能否构造一个公差为正的无限正整数等差数列,其中每一项都不能表示成为两个整数的立方和.

解 由于 $a^3 \equiv 0, \pm 1 (\mathrm{mod}\ 7)$,所以任意两个整数的立方和 $\equiv 0, \pm 1, \pm 2 (\mathrm{mod}\ 7)$,因此我们可以构造两个符合要求的数列 $3+7k, 4+7k$.

1.1.7 设 $n \equiv 2,3 (\mathrm{mod}\ 4)$,则不存在 $1,2,\cdots,2n$ 的排列满足

$$a_1, a_2, \cdots, a_n, b_1, \cdots, b_n, b_i - a_i = i, i = 1, \cdots, n \quad ①$$

证明 如果存在 $1,2,\cdots,2n$ 的某个排列 $a_1, \cdots, a_n, b_1, \cdots, b_n$ 满足 ①,则有

$$\sum_{i=1}^{n} (b_i - a_i) = \sum_{i=1}^{n} i = \frac{n(n+1)}{2} \quad ②$$

另一方面

$$\sum_{i=1}^{n} (b_i + a_i) = \sum_{i=1}^{2n} i = n(2n+1) \quad ③$$

由 ② 和 ③ 得

$$\sum_{i=1}^{n} b_i = \frac{n(5n+3)}{4} \quad ④$$

在 $n \equiv 2,3 (\mathrm{mod}\ 4)$ 时,④ 的左端是整数,右端不是整数,这是矛盾的,故满足 ① 的排列不存在.

注 在 $n \equiv 0,1 (\mathrm{mod}\ 4)$ 时,存在这样的排列,如

$$n = 4,6,1,2,4,7,3,5,8$$

$$n = 5,2,6,7,1,4,3,8,10,5,9$$

1.1.8 在已知数列 1,4,8,10,16,19,21,25,30,43 中,相邻若干数之和能被 11 整除的数组共有多少组.

(中国高中数学联赛,1985 年)

解 记该数列各对应项为 $a_i, i = 1,2,\cdots,10$. 并记

心得 体会 拓广 疑问

$$S_k = a_1 + a_2 + \cdots + a_k$$

由此可计算数列 $S_1, S_2, \cdots, S_{10}$ 为

$$1,5,13,23,39,58,79,104,134,177$$

它们被 11 除的余数依次为

$$1,5,2,1,6,3,2,5,2,1$$

由此可得

$$S_1 \equiv S_4 (\mathrm{mod}\ 11)$$
$$S_1 \equiv S_{10} (\mathrm{mod}\ 11)$$
$$S_4 \equiv S_{10} (\mathrm{mod}\ 11)$$
$$S_2 \equiv S_8 (\mathrm{mod}\ 11)$$
$$S_3 \equiv S_7 (\mathrm{mod}\ 11)$$
$$S_7 \equiv S_9 (\mathrm{mod}\ 11)$$
$$S_3 \equiv S_9 (\mathrm{mod}\ 11)$$

由于 $S_k - S_j (k > j)$ 是数列 $\{a_i\}$ 的相邻项之和，并且当 $S_k \equiv S_j (\mathrm{mod}\ 11)$ 时，$11 \mid S_k - S_j$，于是符合题目要求的数组共有 7 组.

1.1.9 已知三个相邻自然数的立方和是一个自然数的立方. 证明：这三个相邻自然数中间的那个数是 4 的倍数.

证明 下列字母均表示正整数.

由条件，$(x-1)^3 + x^3 + (x+1)^3 = y^3$，$3x(x^2+2) = y^3$，于是 $3 \mid y^3$，故 $3 \mid y$. 设 $y = 3z$，则 $x(x^2+2) = 9z^3$. 显然，$(x, x^2+2) \leqslant 2$.

如果 $(x, x^2+2) = 1$，则 $x = 9u^3$，$x^2 + 2 = v^2$ 或 $x = u^3$，$x^2 + 2 = 9v^3$. 第一种情况下得到 $81u^6 + 2 = v^3$，这是不可能的，因为立方数除以 9 得到的余数只能是 0，± 1. 类似地，第二种情况下得到 $u^6 + 2 = 9v^3$，同样的原因，这也导出矛盾.

现在假设 $(x, x^2+2) = 2$，而 $x(x^2+2) = 9z^3$，则 x, z 均为偶数，故 $8 \mid x(x^2+2)$. 由于 $x^2 + 2$ 不是 4 的倍数，所以 $4 \mid x$.

1.1.10 证明

$$61! + 1 \equiv 0 (\mathrm{mod}\ 71)$$

和

$$63! + 1 \equiv 0 (\mathrm{mod}\ 71)$$

证明 当 p 是一个奇素数时，有

$$(p-1)! + 1 \equiv 0 (\mathrm{mod}\ p) \qquad ①$$

对于整数 $1 \leqslant r \leqslant p-1$，有 $p - j \equiv -j (\mathrm{mod}\ p)$，取 $j = 1, 2, \cdots, r$，再两边相乘，得

$$(p-1)(p-2)\cdots(p-r) \equiv (-1)^r r! \ (\mathrm{mod}\ p) \qquad ②$$

如果存在 r，使

心得 体会 拓广 疑问

$$(-1)^r r! \equiv 1 \pmod{p} \quad ③$$

则由①②③可得

$$-1 \equiv (p-1)! \equiv (p-1)\cdots(p-r)\cdot(p-r-1)! \equiv (-1)^r r!\,(p-r-1)! \equiv (p-r-1)!$$

$$(p-r-1)! + 1 \equiv 0 \pmod{p} \quad ④$$

现在来解本题,因为当 $p=71$ 时 7,9 满足③,即

$$(-1)^7 7! \equiv 1 \pmod{71}$$

和

$$(-1)^9 9! \equiv 1 \pmod{71}$$

所以,由④得到

$$63! + 1 \equiv 0 \pmod{71}$$

和

$$61! + 1 \equiv 0 \pmod{71}$$

注 设 $p=4n+3$ 是一个素数,$l=\frac{1}{2}(p-1)$,r 是 $1,2,\cdots,l$ 中模 p 的平方非剩余的个数,则 $l! \equiv (-1)^r \pmod{p}$.

1.1.11 证明:对于任意正整数 m,均有一个 5 的正整数幂,它的末 m 位数字中任意相邻两个数字具有不同的奇偶性.

证明 首先用归纳法易证对任意正整数 n,$2^{n+1} \parallel 5^{2^n}-1$. 下面对 m 归纳,设已有 5^n 的末 m 位数字奇偶性交替变化,则考虑数 $5^{n+2^{m-1}}$

$$5^{n+2^{m-1}} - 5^n = 5^n(5^{2^{m-1}}-1) \equiv 2^m \pmod{2^{m+1}}$$

$$5^n \equiv 5^{n+2^{m-1}} \pmod{5^{m+1}}$$

即

$$5^{n+2^{m-1}} - 5^n \equiv 5\cdot 10^m \pmod{10^{m+1}}$$

因此这两个数中从右往左数第 $m+1$ 位数字的奇偶性不同,而后 m 位数字的奇偶性均相同,故其中必有一个数符合题意.

1.1.12 设 p 是素数,$p>3$,$n=\frac{2^{2p}-1}{3}$,则

$$2^n - 2 \equiv 0 \pmod{n} \quad ①$$

证明 由

$$n-1 = \frac{2^{2p}-1}{3} - 1 = \frac{4(2^{p-1}+1)(2^{p-1}-1)}{3}$$

得

$$3(n-1) = 4(2^{p-1}+1)(2^{p-1}-1) \quad ②$$

因 $p>3$,$p \mid 2^{p-1}-1$,由②得

$$2p \mid n-1 \quad ③$$

再由③可推得

$$2^{2p}-1 \mid 2^{n-1}-1 \quad ④$$

心得 体会 拓广 疑问

而 $n \mid 2^{2p}-1$，由式④得

$$n \mid 2^{n-1}-1$$

故式①成立.

1.1.13 设 $m,n \in \mathbf{N}^*$，且 $\sqrt{7} > \frac{m}{n}$，求证：$\sqrt{7} - \frac{m}{n} > \frac{1}{mn}$.

（罗马尼亚，1978年）

证明 只需证明，由 $\sqrt{7}n - m > 0$ 可以推出 $\sqrt{7}n - m > \frac{1}{m}$，其中 $m,n \in \mathbf{N}^*$. 如果 $\sqrt{7}n - m = 1$，则 $\sqrt{7} = \frac{1+m}{n}$ 为有理数，不可能.

设 $0 < \sqrt{7}n - m < 1$. 注意，因为 m^2 被7除的余数不能是6或5. 事实上

$$(7k)^2 \equiv 0 \pmod 7, \quad (7k \pm 1)^2 \equiv 1 \pmod 7$$

$$(7k \pm 2)^2 \equiv 4 \pmod 7, \quad (7k \pm 3)^2 \equiv 2 \pmod 7$$

所以 $7n^2 - m^2 = (\sqrt{7}n - m)(\sqrt{7}n + m)$ 不能是1或2，因此 $7n^2 - m^2 \geqslant 3$. 由于

$$3m \geqslant 2m + 1 > 2m + (\sqrt{7}n - m) = \sqrt{7}n + m$$

所以 $\sqrt{7}n - m \geqslant \frac{3}{\sqrt{7}nm} > \frac{1}{m}$. 证毕.

1.1.14 已知 p 是一个大于5的素数，证明：至少存在两个不同素数 q_1 和 q_2 满足 $1 \leqslant q_1,q_2 < p-1$，且 $a_i^{p-1} \not\equiv 1 \pmod{p^2}$ $(i=1,2)$.

（新加坡，2004年）

证明 首先证明引理：若 $a^b \not\equiv 1 \pmod c$，则必存在素数 $q \mid a$，且 $q^b \not\equiv \pmod c$. 设 $a = p_1^{a_1} \cdot p_2^{a_2} \cdot \cdots \cdot p_t^{a_t}$，假设结论不成立，则 $p_i^b \equiv 1 \pmod c$ $(i=1,2,\cdots,t)$，易得 $a^b \equiv 1 \pmod c$，矛盾，故存在素数 $q \mid a$，使得 $q^b \not\equiv 1 \pmod c$.

回到原题，考虑 $(p-1)^{p-1}$，$(p+1)^{p-1}$，$(2p-1)^{p-1}$，$(2p+1)^{p-1}$，显然由二项式定理展开可知这4个数在模 p^2 下的余数均不为1.

所以存在 $q_1 \mid p-1$ $(q_1 < p-1)$，使得 $q_1^{p-1} \not\equiv 1 \pmod{p^2}$.

若 $q_1 \neq 2$，由引理存在 $q_2 \mid p+1$，且 $q_2^{p-1} \not\equiv 1 \pmod{p^2}$.

又因为 $(q_1,q_2) \leqslant (p+1,p-1) = 2$，而 q_1 和 q_2 为素数，所以 $q_1 \neq q_2$，则 q_1,q_2 即为所求.

心得 体会 拓广 疑问

若 $q_1=2$,那么由 $2p-1,2p+1$ 中必有一数被3整除,则由引理存在 $q_2 \mid 2p-1$ 或 $2p+1$,且 $q_2^{p-1} \not\equiv 1 \pmod{p^2}$,易得 q_2 为奇数,且 $q_2 \leqslant \frac{2p+1}{3} < p-1$,则 q_1,q_2 即为所求,命题得证.

1.1.15 设 $p>3$,p 是素数,则对任意的 a,b 满足

$$ab^p - ba^p \equiv 0 \pmod{6p} \quad ①$$

证明 因为

$$b^p - b = b(b^{p-1}-1) = b((b^2)^{\frac{p-1}{2}} - 1) =$$

$$b(b^2-1)((b^2)^{\frac{p-1}{2}-1} + \cdots + 1)$$

所以

$$b(b^2-1) \mid b^p - b$$

而 $6 \mid b(b^2-1)$,上式给出 $6 \mid b^p-b$,又因 $(6,p)=1$,$b^p-b \equiv 0 \pmod{p}$,故

$$6p \mid b^p - b$$

由此可得

$$a(b^p-b) \equiv 0 \pmod{6p} \quad ②$$

类似可得

$$b(a^p-a) \equiv 0 \pmod{6p} \quad ③$$

由②和③便得到式①.

1.1.16 求证:对任意 $n \in \mathbf{Z}^*$,$19 \cdot 8^n + 17$ 是合数.

证明 这里恒设 $k \in \mathbf{Z}^*$. 如果 $n=2k$,则

$$19 \cdot 8^{2k} + 17 = 18 \cdot 8^{2k} + 1 \cdot (1+63)^k + (18-1) \equiv 0 \pmod{3}$$

如果 $n=4k+1$,则

$$19 \cdot 8^{4k+1} + 17 = 13 \cdot 8^{4k+1} + 6 \cdot 8 \cdot 64^{2k} + 17 =$$

$$13 \cdot 8^{4k+1} + 39 \cdot 64^{2k} + 9 \cdot (1-65)^{2k} +$$

$$(13+4) \equiv 0 \pmod{13}$$

如果 $n=4k+3$,则

$$19 \cdot 8^{4k+3} + 17 = 15 \cdot 8^{4k+3} + 4 \cdot 8^3 \cdot 64^{2k} + 17 =$$

$$15 \cdot 8^{4k+3} + 4 \cdot 510 \cdot 64^{2k} + 4 \cdot 2(1-65)^{2k} +$$

$$(25-8) \equiv 0 \pmod{5}$$

由此可见,对任意 $n \in \mathbf{Z}^*$,$19 \cdot 8^n + 17$ 至少被3,13或5之一整除.

1.1.17 设 k 是正整数，证明：存在无限多个形如 $n \cdot 2^k - 7$ 的完全平方数，其中 n 为正整数.

（罗马尼亚，1995 年）

证明 首先证明，对任给的 $k \in \mathbf{N}^*$，存在正整数 a_k，使得 $a_k^2 \equiv -7 \pmod{2^k}$. 对 k 用数学归纳法. 由直接观察可知，当 $k \leqslant 3$ 时，取 $a_k = 1$ 便可满足条件，设对某个 $k > 3$，有 $a_k^2 \equiv -7 \pmod{2^k}$. 下面考虑 a_k^2 模 2^{k+1} 的余数，易知 $a_k^2 \equiv -7 \pmod{2^{k+1}}$ 或 $a_k^2 \equiv 2^k - 7 \pmod{2^{k+1}}$. 对于前者，可取 $a_{k+1} = a_k$，对后者可取 $a_{k+1} = a_k + 2^{k-1}$. 事实上，由于 $k \geqslant 3$ 且 a_k 是奇数，所以

$$a_{k+1}^2 = a_k^2 + 2^k a_k + 2^{2k-2} \equiv a_k^2 + 2^k a_k \equiv$$
$$a_k^2 + 2^k \equiv -7 \pmod{2^{k+1}}$$

最后容易看出，序列 $\{a_k\}$ 没有最大元素，因为可以要求对任何 k，$a_k^2 \geqslant 2^k - 7$，因而 $\{a_k\}$ 包含无穷多个不同的值.

1.1.18 证明：有无限多个形如 5^n 的数，在它们的十进制写法中至少连续出现 1 976 个 0.

（越南，1976 年）

证明 我们证明，对任意 $k \in \mathbf{N}^*$，有无限多个 $m \in \mathbf{N}^*$，使得 $5^m \equiv 1 \pmod{2^k}$，事实上，由 Dirichlet 原理，在 $5^0, 5^1, 5^2, \cdots, 5^{2^k}$ 中至少有两个 5^p 与 5^q，$p > q$，它们被 2^k 除的余数相同. 于是它们的差 $5^p - 5^q = 5^q(5^{p-q} - 1)$ 被 2^k 整除. 因而 $5^{p-q} - 1$ 以及 $5^{r(p-q)} - 1$，$r \in \mathbf{N}^*$，都被 2^k 整除，于是对每个 $m = r(p-q)$，$r \in \mathbf{N}^*$ 有

$$5^m \equiv 1 \pmod{2^k}, 5^{m+k} \equiv 5^k \pmod{10^k}$$

即 5^{m+k} 的末尾 k 个数字构成 5^k 的十进制表示，取 $k \in \mathbf{N}^*$，使得 $2^k > 10^{1\,976}$，则

$$5^k = \frac{10^k}{2^k} < 10^{k-1\,976}$$

即 5^k 的十进制写法中至多含有 $k - 1\,976$ 个数字. 因此 5^{m+k} 的末尾 k 个数字中，非零的数字只能是最后那 $k - 1\,976$ 个，而其余（接连出现的）1 976 个数字都是 0. 结论证毕.