

全国奥数总领队担纲 金牌教练精心打造

高中数学竞赛 培优教程

(专题讲座)

李胜宏 李名德 主编

浙江大学出版社

高中数学竞赛培优教程

(专题讲座)

主 编 李胜宏 李名德
编 委 (按姓氏笔画为序)
王祖樾 叶景梅
李名德 李胜宏
徐士英 瞿维建

浙 江 大 学 出 版 社

图书在版编目(CIP)数据

高中数学竞赛培优教程:专题讲座 / 李胜宏, 李名德
主编. —杭州:浙江大学出版社, 2003.4
ISBN 7-308-03241-8

I. 高... II. ①李...②李... III. 数学课—高中—
教学参考资料 IV. G631.603

中国版本图书馆 CIP 数据核字(2003)第 000770 号

出版发行 浙江大学出版社
(杭州浙大路 38 号 邮政编码 310027)
(E-mail: zupress@mail. hz. zj. cn)
(网址: <http://www.zjupress.com>)

责任编辑 杨晓鸣
排 版 浙江大学出版社电脑排版中心
印 刷 浙江大学印刷厂
开 本 787mm×960mm 1/16
印 张 23
字 数 460 千字
版 印 次 2003 年 4 月第 1 版 2006 年 3 月第 8 次印刷
印 数 37001—42000
书 号 ISBN 7-308-03241-8/G·592
定 价 26.00 元

前 言

我国自 1985 年首次参加国际中学生数学奥林匹克竞赛以来,连年取得了优异的成绩,多次获得团体总分第一,此事备受世界各国的关注,同时也激发了我国广大中学生对数学的热情与兴趣。这无疑对培养人才起到了积极的推动作用。我省在浙江省数学会的积极组织和推动下,自 1997 年至今每年假期举办为期 1 至 2 周的浙江省数学夏令营活动,邀请具有丰富教学经验的高级中学的特级教师、高级教师和大学的教授、专家授课。这项活动取得了显著的成绩。近几年来,我省在全国高中数学联合竞赛中成绩屡屡名列前茅。

为了满足广大中学生对数学奥林匹克竞赛指导教程的需要,以及为从事中学的数学工作者指导学生提供有益的参考资料,我们邀请历年担任浙江省数学夏令营授课的大学教授,中学特级教师、高级教师,结合新编的高中数学教材内容,编写了针对全国高中数学联合竞赛(一、二试)要求的高中数学竞赛同步辅导丛书。丛书是在历年(自 1997 年始)数学夏令营授课讲义的基础上,经修改、补充、完善而成。丛书由浙江大学教授、博士生导师、全国数学奥林匹克竞赛总领队李胜宏和浙江大学教授李名德先生主编。

本书是按全国高中数学联合竞赛“加试赛”(二试)的要求编写的,内容包括加试赛要求的全部知识,并分为若干个专题论述。本书精选了大量的典型例题,并作了详尽的讲解,旨揭示解题规律,提高学生分析问题和解决问题的能力。每个章节都提供了足量的练习题,供学生课外训练。这些练习题只给出了简单的提示,目的是培养学生独立思考问题的能力和探求精神。

参加本书编写的人员有(按姓氏笔画为序):杭州电子工学院教授王祖樾(第六章),浙江教育学院教授叶景梅(第一、二章),浙江大学教授李名德(第三、四章),浙江大学教授李胜宏(第五、九章),中国计量学院教授徐士英(第七章),杭州师范学院副教授瞿维建(第八章)。

本书第五次重印时,增加了部分练习题,对部分习题补充了参考答案,其中第五章的习题提示和第九章习题及提示由振云先生提供。

编 者

第一章 数论的基本知识	(1)
§ 1.1 整数与余数	(1)
§ 1.2 最大公因数与最小公倍数	(4)
§ 1.3 素数、算术基本定理	(6)
§ 1.4 几个数论函数	(9)
§ 1.5 同余的概念与性质	(12)
第二章 数学奥林匹克中的数论问题专题讲座	(17)
§ 2.1 整除性问题	(17)
§ 2.2 整数、素数、完全平方数的判定	(22)
§ 2.3 解不定方程的一些方法	(28)
§ 2.4 有关数论的竞赛题的一些常用入手方法	(37)
第三章 数列与归纳法	(52)
§ 3.1 预备知识	(52)
§ 3.2 有关数列的竞赛题举例	(62)
第四章 不等式与最值	(70)
§ 4.1 预备知识	(70)
§ 4.2 利用著名不等式解题	(74)
§ 4.3 利用和式的变换解题	(81)
§ 4.4 利用递推关系(包括数学归纳法)解题	(93)
§ 4.5 用其他方法解题	(96)
第五章 多项式	(104)
§ 5.1 基本概念	(104)
§ 5.2 多项式的整除	(106)
§ 5.3 最大公因式	(109)
§ 5.4 因式分解	(112)
§ 5.5 根与系数的关系	(115)
§ 5.6 复数与多项式	(118)

§ 5.7	例题选讲	(121)
§ 5.8	整系数多项式	(133)
§ 5.9	多项式的差分	(137)
§ 5.10	拉格朗日(Lagrange)插值多项式	(144)
§ 5.11	多元多项式	(153)
第六章	函数方程与竞赛题解题思想方法	(170)
§ 6.1	函数方程引入	(170)
§ 6.2	决定周期函数的函数方程	(172)
§ 6.3	估算函数值与界的问题	(173)
§ 6.4	连续型函数方程	(178)
§ 6.5	离散型函数方程	(184)
§ 6.6	函数方程的构造性解答	(192)
§ 6.7	竞赛题解题思想方法	(196)
第七章	组合数学的解题思想和典型问题	(214)
§ 7.1	组合数学常用的解题思想	(214)
§ 7.2	组合数学的几类典型问题	(238)
第八章	图论与数学竞赛	(259)
§ 8.1	引言	(259)
§ 8.2	图论基本知识介绍	(262)
§ 8.3	如何将图论结果改造成竞赛试题	(268)
§ 8.4	以图论为背景的竞赛试题分类举例	(270)
第九章	初等几何	(285)
§ 9.1	圆的基本性质	(285)
§ 9.2	圆幂和根轴	(290)
§ 9.3	三角形的“五心”	(299)
§ 9.4	重要定理及其应用	(308)
§ 9.5	常用解题方法	(316)
附录	参考答案	(333)

第一章 数论的基本知识

在本章中,我们将介绍数学竞赛所涉及的一些初等数论基本知识,其中包括一些概念、定理或性质.由于我们的目标仅仅是使用这些知识,因而我们将不追求理论的完备性,在多数情况下,有关定理和性质是不加证明的.

本书中,我们将用 \mathbf{Z} 表示整数全体所成的集合

$$\mathbf{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\},$$

而用拉丁字母 a, b, c 等表示整数.我们将不再重复人们已熟知的整数的一些知识,如整数四则运算的性质,整数的有序性等等.但应指出一个易被忽视的重要性质——最小(大)整数原理:有下(上)界的非空整数集,必有最小(大)元素.

§ 1.1 整数与余数

众所周知,加、减、乘三种运算在集 \mathbf{Z} 中是封闭的,也就是说,两整数的和、差、积仍然是整数.然而,用一非零整数去除另一整数,所得的商未必是整数.这就导致了整除性的讨论.这种讨论的基础是带余除法定理.

定理 1(带余除法定理) 若 $a, b \in \mathbf{Z}, b \neq 0$, 则存在惟一的整数对 q 及 r , 满足

$$a = bq + r, \quad 0 \leq r < |b|. \quad (1.1)$$

(1.1)式中的整数 q 称为 a 被 b 除所得的不完全商(简称为商),非负整数 r 称为 a 被 b 除所得的余数.当余数 $r=0$,即 $a=bq$ 时,我们称 a 被 b 整除,记为 $b|a$;当 $r \neq 0$ 时,称 a 不能被 b 整除,记为 $b \nmid a$;当 $b|a$ 时,称 b 是 a 的因数, a 是 b 的倍数.应强调指出,余数 r 必须满足 $0 \leq r < |b|$.例如,虽然有

$$12 = 5 \times 1 + 7, \quad 12 = 5 \times 3 + (-3),$$

但 $7, -3$ 都不是 12 被 5 除所得的余数.

【例 1.1】 求所有被 4 除余 1 的两位整数之和 S .

【解】 被 4 除余 1 的一切正整数可写成如下形式:

$$4q + 1, \quad q = 0, 1, 2, \dots$$

命题中限制这些数是两位数,故 $10 \leq 4q + 1 < 100$,于是得 $3 \leq q \leq 24$,从而由等差

数列求和公式即可得 $S = \sum_{q=3}^{24} (4q+1) = 1210$.

由整除的定义可直接得到下列基本性质:

性质 1° 若 $b|a$, 则 $\pm b|\pm a$.

根据这一性质, 我们可以限制在正整数的范围内来讨论整除性问题. 特别地, 关于数的因数, 我们只需考虑正因数.

性质 2° 若 $a|b, b|c$, 则 $a|c$.

性质 3° 若 $a|a_i, i=1, 2, \dots, k$, 则

$$a|(c_1a_1 + c_2a_2 + \dots + c_ka_k),$$

这里 c_1, c_2, \dots, c_k 是任意整数.

由性质 3° 可得如下结论: 各项均代表整数的等式中, 除一项外, 其余项均可被某数整除, 则此项也可被该数整除. 这一结论是讨论数论竞赛题的重要手段之一: 在观察有关整数的等式时, 首先应看一看式中是否有很多项同时被某数整除. 如果有, 则把剩下的项看成一项, 它也被该数整除.

【例 1.2】 试求方程 $2x^2 + y^2 = 3x^2y$ 的正整数解.

【解】 显然项 $2x^2, 3x^2y$ 都有因数 x^2 , 因而得 $x^2|y^2$, 从而 $x|y$. 由 x, y 是正整数知可设 $y = tx, t$ 是正整数. 以此代入方程, 得

$$2x^2 + t^2x^2 = 3x^3t, \quad 2 + t^2 = 3xt.$$

同理, 又有 $t|2$. 因而只能是 $t = 1, 2$. 据此不难得到两组解 $x = y = 1; x = 1, y = 2$.

依整除的定义, 为了证明 $b|a$, 只须证明存在整数 q , 或直接找出具体的整数 q , 使 $a = bq$ 成立. 这是一种最直接的常用方法.

【例 1.3】 试证任意一个整数与它的各位数码字之和的差能被 9 整除, 且这个数与其数码字作任意顺序调换后所成的整数的差, 也能被 9 整除.

【证明】 不妨设整数 $m > 0$, 它的十进位表示是

$$m = a_1 + 10a_2 + \dots + 10^{n-1}a_n,$$

这里 a_1, a_2, \dots, a_n 是数码字, 则

$$m - (a_1 + a_2 + \dots + a_n) = 9(a_2 + 11a_3 + \dots + \underbrace{11\dots 1}_{n-1\uparrow}a_n).$$

因而 $9|(m - (a_1 + a_2 + \dots + a_n))$.

又设 b_1, b_2, \dots, b_n 是 a_1, a_2, \dots, a_n 的另一个排列,

$$m' = b_1 + 10b_2 + \dots + 10^{n-1}b_n.$$

若记 $\sigma = a_1 + a_2 + \dots + a_n$, 则 $\sigma = b_1 + b_2 + \dots + b_n$. 于是由前面的证明可知

$$9|(m - \sigma), \quad 9|(m' - \sigma).$$

即 $m - \sigma = 9q, m' - \sigma = 9q'$, 于是 $m - m' = 9(q - q')$, 从而 $9|(m - m')$.

式子 $a = bq$ 实际上是把整数 a 分解为两个整数 b 与 q 的乘积. 因此, 在讨论整除性问题时, 常常使用各种因式分解公式. 除了中学课本常见的公式外, 我们还应注意下列公式:

对于任意正整数 n , 有

$$a^n - b^n = (a - b)M_1, \quad (1.2)$$

这里 $M_1 = a^{n-1} + a^{n-2}b + \cdots + ab^{n-2} + b^{n-1} \in \mathbf{Z}$.

当 n 为正奇数时, 有

$$a^n + b^n = (a + b)M_2, \quad (1.3)$$

这里 $M_2 = a^{n-1} - a^{n-2}b + \cdots + (-1)^{n-2}ab^{n-2} + (-1)^{n-1}b \in \mathbf{Z}$.

此外, 由二项式公式

$$(a + b)^n = a^n + C_n^1 a^{n-1}b + \cdots + C_n^{n-1} ab^{n-1} + b^n = a(a^{n-1} + C_n^1 a^{n-2}b + \cdots + C_n^{n-1} b^{n-1}) + b^n,$$

可得

$$(a + b)^n = aM_3 + b^n, M_3 \in \mathbf{Z}. \quad (1.4)$$

【例 1.4】 试证 $1999 | (1998^{1998} + 2000^{2000} - 2001)$.

【证明】 由公式(1.4)知

$$1998^{1998} = (1999 - 1)^{1998} = 1999M + 1,$$

$$2000^{2000} = (1999 + 1)^{2000} = 1999N + 1,$$

这里 $M, N \in \mathbf{Z}$. 于是

$$1998^{1998} + 2000^{2000} - 2001 = 1999M + 1999N - 1999 = 1999(M + N - 1),$$

从而 $1999 | (1998^{1998} + 2000^{2000} - 2001)$.

【例 1.5】 设 n 是任意正整数, m 是任意正奇数, $S = 1^m + 2^m + \cdots + n^m$, 试证 $(n+2) \nmid S$.

【证明】 把 S 写成由小到大及由大到小的两种和式, 然后错位直式相加如下:

$$\begin{array}{r} S = 1^m + 2^m + \cdots + k^m \quad \quad \quad + \cdots + n^m \\ +) S = \quad \quad \quad n^m + \cdots + (n - k + 2)^m + \cdots + 2^m + 1^m \\ \hline \end{array}$$

$$2S = 1 + (n+2)M_2 + \cdots + (n+2)M_k + \cdots + (n+2)M_n + 1,$$

这里我们利用了 m 是正奇数, 从而由公式(1.3)知

$$k^m + (n - k + 2)^m = (n+2)M_k, \quad k = 2, 3, \cdots, n.$$

这样, 就有 $2S = 2 + (n+2)(M_2 + \cdots + M_k + \cdots + M_n)$.

若 $(n+2) | S$, 由上式将得 $(n+2) | 2$. 但 $n+2 > 2$, 这是矛盾的, 故 $(n+2) \nmid S$.

最后, 我们要说明带余除法定理的(1.1)式, 它指出了全体整数可按照被某数 b 除所得的余数进行分类. 例如, 当 $b = 2$ 时, 整数可分成偶数和奇数两类, 并依次写成:

$$2k, 2k-1, k \in \mathbf{Z}$$

两种形状. 当 $b=3$ 时, 整数可分成三类, 写成

$$3k, 3k+1, 3k+2, k \in \mathbf{Z}.$$

【例 1.6】 试证对于任意整数 x , 有 $3|(2x^3+3x^2+x)$.

【证明】 注意到 $2x^3+3x^2+x=2x(x^2-1)+3(x+1)$. 因而, 只需证明 $3|2x(x^2-1)$.

当 $x=3k$ 时, 有 $2x(x^2-1)=6k(x^2-1)$;

当 $x=3k+1$ 时, 有 $2x(x^2-1)=2x(x-1)(x+1)=6kx(x+1)$;

当 $x=3k+2$ 时, 有 $2x(x^2-1)=2x(x-1)(x+1)=6(k+1)x(x-1)$.

因而不论哪一种情况, 均有 $3|2x(x^2-1)$, 从而命题结论正确.

练习题

1. 设 $3|(2a+b)$, 试证 $9|(8a^2-10ab-7b^2)$.
2. 设 $(m-p)|(mn+pq)$, 试证 $(m-p)|(mq+np)$.
3. 设 n 为正偶数, 试证 $(2^n-1)|(3^n-1)$.
4. 设 m, n 是正整数, $10|(3^m+1)$, 试证 $10|(3^{m+4n}+1)$.
5. 设 a, b 是正整数, n 是非负整数, 试证若 $a^n|b$, 则 $a^{n+1}|((a+1)^b-1)$.
6. 设 $f(x)$ 是整系数多项式, 且存在整数 k , 使得 $f(0), f(1), \dots, f(k-1)$ 都不能被 k 整除, 试证 $f(x)$ 无整数根.
7. 设 $3|(a^2+b^2)$, 试证 $3|a$ 且 $3|b$.
8. 设 n, k 是正整数, 试证 n^k 与 n^{k+4} 的个位数字相同.

§ 1.2 最大公因数与最小公倍数

本节我们仅仅讨论两个整数的最大公因数与最小公倍数. 但这两个概念是可以推广到多于两个数的情况的.

若 a, b 是两个不全为零的整数, 且 $d|a, d|b$, 则称 d 是 a, b 的公因数. 公因数中的最大者, 称为 a, b 的最大公因数, 记为 (a, b) . 若 $(a, b)=1$, 则称 a, b 互素.

若 a, b 是两个非零整数, 且 $a|M, b|M$, 则称 M 是 a, b 的公倍数. 公倍数中的最小正数, 称为 a, b 的最小公倍数, 记为 $[a, b]$.

由定义易知

$$(a, b) = (|a|, |b|), \quad [a, b] = [|a|, |b|].$$

因此,我们可限制在正整数的范围内讨论最大公因数与最小公倍数的问题.下文中,字母一般代表正整数.

关于最大公因数和最小公倍数,有如下性质:

性质 1° 设 $a = bq + c$, 则 $(a, b) = (b, c)$.

这一性质可作如下变形:把 $c = a - bq$ 代入上式,可得

$$(a, b) = (a - bq, b), \quad (1.5)$$

这就是说,在计算 (a, b) 时,可用 b 的任意倍数 bq 去减(加) a . 这种方法在计算上是方便的.例如 $(n+1, n) = (n+1-n, n) = (1, n) = 1$, 由此可知相邻两整数必互素.

【例 1.7】 (IMO) 试证 $\frac{21n+4}{14n+3}$ 是既约分数.

【证明】 由(1.5)式知

$$(21n+4, 14n+3) = (7n+1, 14n+3) = (7n+1, 1) = 1.$$

这样,所给分式的分子与分母互素,因而分式是既约分数.

性质 2° a, b 的公因数全体所成的集合,与 (a, b) 的因数全体所成的集合相同.

性质 3° $(ac, bc) = |c|(a, b)$.

性质 4° 若 a, b 不全为零,则必存在整数 s, t , 使 $as + bt = (a, b)$.

性质 5° $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$.

这一性质也可改写如下:设 $(a, b) = d$, 则可令

$$a = a_1d, \quad b = b_1d, \quad (a_1, b_1) = 1.$$

这样一来,对于一般的整数 a, b 的讨论可转为对于互素的整数 a_1, b_1 的讨论.由于互素的两数具有许多特殊的性质可供利用,因而这种转换是十分有用的方法和技巧.

性质 6° 若 b, c 不全为零, $(a, c) = 1$, 则 $(ab, c) = (b, c)$.

性质 7° 若 $(a, b) = 1, b|ac$, 则 $b|c$.

性质 8° 若 $(a, b) = 1, a|c, b|c$, 则 $ab|c$.

性质 9° 若 $(a_i, b_j) = 1, i = 1, 2, \dots, m, j = 1, 2, \dots, n$, 则

$$(a_1a_2 \cdots a_m, b_1b_2 \cdots b_n) = 1.$$

特别地,若 $(a, b) = 1$, 则 $(a^m, b^n) = 1$.

【例 1.8】 若 $17|(2a+3b)$, 试证 $17|(9a+5b)$.

【证明】 注意到 $2(9a+5b) = 9(2a+3b) - 17b$, 于是 $17|2(9a+5b)$. 但 $(17, 2) = 1$, 由性质 7° 即得 $17|(9a+5b)$.

【例 1.9】 设 k 为正奇数, 试证 $(1+2+\cdots+9)|(1^k+2^k+\cdots+9^k)$.

【证明】 记 $S = 1^k+2^k+\cdots+9^k$, 则 $2S$ 可分别表为

$$2S = (1^k+9^k) + (2^k+8^k) + \cdots + (9^k+1^k) = 10M_1,$$

$$2S = (0^k + 9^k) + (1^k + 8^k) + \cdots + (9^k + 0^k) = 9M_2,$$

这里 $M_1, M_2 \in \mathbf{Z}$, 于是 $9|2S, 10|2S$. 但 $(9, 10) = 1$, 故由性质 8° 知 $90|2S, 45|S$.

【例 1.10】 设 n, a 是正整数, 若 $\sqrt[n]{a}$ 不是整数, 就必是无理数.

【证明】 设 $\sqrt[n]{a}$ 是非整数的有理数, 则可设 $\sqrt[n]{a} = \frac{c}{b}, b > 1, (b, c) = 1$, 于是 $a = \frac{c^n}{b^n}$. 因 $(b, c) = 1$, 故由性质 9° 知 $(b^n, c^n) = 1$. 但 $b^n > 1$, 因而 $b^n \nmid c^n$. 这与 $\frac{c^n}{b^n} = a$ 是整数相矛盾. 命题证毕.

性质 10° $[a, b] = \frac{ab}{(a, b)}$, 特别地, 若 $(a, b) = 1$, 则 $[a, b] = ab$.

练习题

1. 若 $(6n+5, 7n+3) \neq 1$, 试求出最大公因数, 并指出此时 n 应满足的条件.
2. 设 m, n 是正整数, $2 \nmid m$, 试证 $(2^m - 1, 2^n + 1) = 1$.
3. 设 $M_n = 2^n - 1$, 试证 $(M_m, M_n) = 1$ 的充要条件是 $(m, n) = 1$.
4. 设 a, b 是不全为零的整数, 一切形如 $ax + by (x, y \in \mathbf{Z})$ 的数中的最小正数是 d , 试证 $d = (a, b)$.
5. 记 $F_n = 2^{2^n} + 1$, 试证 $(F_m, F_n) = 1$, 这里 $m \neq n$.

§ 1.3 素数、算术基本定理

根据数的正因数的个数, 可将所有的正整数分为三类:

1. 只有一个正因数的正整数. 显然, 这种数只有一个, 就是单位数 1.
2. 恰有两个正因数的正整数, 这种数称为素数, 如 2, 3, 5, 7 等等. 显然, 这两个正因数就是 1 与该数本身.
3. 至少有三个正因数的正整数, 这种数称为合数, 如 4, 6, 10 等等.

依上述定义, 1 既不是素数, 也不是合数. 2 是惟一的偶素数. 今后, 我们常用 p 代表素数.

关于素数, 有下列性质:

性质 1° 设 a 是整数, p 是素数, 则 $p \nmid a$ 的充要条件是 $(a, p) = 1$.

这一性质表明整数 a 与素数 p 之间只有两种关系, 或者有整除关系 $p|a$, 否则就有互素关系 $(a, p) = 1$.

性质 2° 设 a_1, a_2, \dots, a_n 是整数, p 是素数. 若 $p \mid a_1 a_2 \cdots a_n$, 则至少存在一个 $i (1 \leq i \leq n)$, 使 $p \mid a_i$.

性质 3° 设整数 $a > 1$, 则 a 的大于 1 的最小正因数 p 是素数, 且当 a 是合数时, $p \leq \sqrt{a}$.

性质 4° 素数全体所成的集是无限集.

【证明】 若素数集是有有限集, 则可设集

$$P = \{p_1, p_2, \dots, p_k\}$$

是全体素数所成的集. 这时, 令 $N = p_1 p_2 \cdots p_k + 1$, 显然整数 $N > 1$. 于是由性质 3° 知 N 的大于 1 的最小正因数 p 是素数, 故 $p \in P$. 这样, p 就是 p_1, p_2, \dots, p_k 中的某一个, 因而 $p \mid p_1 p_2 \cdots p_k$. 注意到 p 是 N 的因数, 故 $p \mid N$. 于是

$$p \mid N - p_1 p_2 \cdots p_k = 1,$$

这是不可能的. 从而素数集是无限集.

上述证明是构造性的证明方法, 我们构造了一个特殊形状的数 $N = p_1 p_2 \cdots p_k + 1$, 然后通过讨论 N 的素因数 p , 找出了矛盾. 构造性方法是数论命题的常用解题方法之一, 现再举一例.

【例 1.11】 试证对于任意正整数 n , 存在相继的 n 个自然数皆为合数.

【证明】 我们考虑一个自然数 N , 则相继的 n 个自然数是

$$N, N+1, \dots, N+(n-1).$$

但要判断 $N+1$ 是素数还是合数是十分困难的, 因而不列入考虑. 因此, 我们可以把所需要的 N 个数往后顺移, 转而观察

$$N+2, N+3, \dots, N+(n+1). \quad (1.6)$$

为使 $N+2$ 是合数, 可要求 2 是 N 的因数; 要使 $N+3$ 是合数, 可要求 3 是 N 的因数……最后要使 $N+(n+1)$ 是合数, 可要求 $n+1$ 是 N 的因数. 这样一来, 最简单的构造就是取 $N = 2 \cdot 3 \cdots (n+1) = (n+1)!$, 此时, n 个相继的自然数 (1.6) 就全部都是合数.

要找一个式子, 使这个式的值总是素数, 这是不可能的. 然而, 寻找使某些式子的值为素数的必要条件, 还是有可能的.

【例 1.12】 设 $a^n - 1 (n > 1)$ 是素数, 试证 $a = 2$, 且 n 是素数.

【证明】 当 $a \geq 3$ 时, 有

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1),$$

其中一个因式 $a-1 \geq 2$, 而由 $n > 1$ 知另一因式有

$$a^{n-1} + \cdots + a + 1 \geq a + 1 \geq 4,$$

从而 $a^n - 1$ 是合数. 因而要使 $a^n - 1$ 是素数, 就必须 $a = 2$.

其次, 若 n 是合数, 则有 $n = bc, b > 1, c > 1$. 记 $a^b = d$, 则 $d \geq 2^2 = 4$, 于是

$$a^n - 1 = d^c - 1 = (d-1)(d^{c-1} + \cdots + d + 1).$$

其中 $d-1 > 1, d^{c-1} + \cdots + d + 1 \geq d + 1 > 1$, 因而 $a^n - 1$ 也是合数. 从而要使 $a^n - 1$ 是素数, n 就必须是素数.

形如 $2^n - 1$ 的数称为梅森(Mersenne)数, 记作 M_n . 人们常通过它来得到大素数. 截至 1983 年止, 已知的最大素数是 M_{86243} .

定理 2(算术基本定理) 任何一个大于 1 的整数均可分解为素数的乘积, 若不考虑素数相乘的前后顺序, 则分解式是惟一的.

例如, $24 = 2 \times 2 \times 2 \times 3$. 一个整数分解成素数的乘积时, 其中有些素数可能重复出现. 例如上面 24 的分解式中, 2 出现了三次. 把分解式中相同的素数的积写成幂的形式, 我们就可把大于 1 的整数 a 写成

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \quad \alpha_i > 0, \quad i = 1, 2, \cdots, s. \quad (1.7)$$

上述式子称为 a 的标准分解式. 这样, 算术基本定理也可表述为大于 1 的整数的标准分解式是惟一的(不考虑乘积的先后顺序).

推论 1 若 a 的标准分解式是(1.7), 则 d 是 a 的正因数的充要条件是

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}, \quad 0 \leq \beta_i \leq \alpha_i, \quad i = 1, 2, \cdots, s. \quad (1.8)$$

应说明的是(1.8)不能称为 d 的标准分解式, 其原因是其中某些 β_i 可能取零值(d 可能不含某个素因数 p_i , 因而 $\beta_i = 0$).

推论 2 设 $a = bc$, 且 $(b, c) = 1$, 若 a 是整数的 k 次方, 则 b, c 也是整数的 k 次方. 特别地, 若 a 是整数的平方, 则 b, c 也是整数的平方.

【例 1.13】 设正整数 $m, n > 1, (m, n) = 1$, 试证 $\left(\frac{m+n}{m}\right)^{\frac{m}{n}}$ 是无理数.

【证明】 若 $\left(\frac{m+n}{m}\right)^{\frac{m}{n}}$ 是有理数, 则可设 $\left(\frac{m+n}{m}\right)^{\frac{m}{n}} = \frac{b}{a}$, $(a, b) = 1$, 故 $(m+n)^m a^n = m^m b^n$.

因 $(m+n, m) = (n, m) = 1$, 故 $((m+n)^m, m^m) = 1$. 于是由 $m^m | (m+n)^m a^n$ 知 $m^m | a^n$. 同理, 由 $(a^n, b^n) = 1$ 可得 $a^n | m^m$. 这样, 由上式即得 $(m+n)^m = b^n, m^m = a^n$.

现在来观察第二个等式 $m^m = a^n$. 因 $m > 1$, 故必有 $a > 1$, 且 m 与 a 有相同的素因数. 设它们的标准分解式分别是 $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, $m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$. 于是

$$p_1^{n\alpha_1} p_2^{n\alpha_2} \cdots p_s^{n\alpha_s} = p_1^{m\beta_1} p_2^{m\beta_2} \cdots p_s^{m\beta_s}.$$

既然上式左右两边相等, 由算术基本定理关于标准分解式惟一性的结论知

$$n\alpha_i = m\beta_i, \quad i = 1, 2, \cdots, s.$$

再由 $(m, n) = 1$ 可得 $m | \alpha_i$, 从而有 $\alpha_i = mt_i, t_i \in \mathbf{Z}, i = 1, 2, \cdots, s$. 代入前面式子, 又可得 $\beta_i = nt_i, i = 1, 2, \cdots, s$.

这样, 若记 $c = p_1^{t_1} p_2^{t_2} \cdots p_s^{t_s}$, 就有 $m = p_1^{nt_1} p_2^{nt_2} \cdots p_s^{nt_s} = c^n, c > 1$.

对等式 $(m+n)^m = b^n$ 作同样的讨论,可证明存在 $d \in \mathbf{Z}$, 使

$$m+n = d^n, \quad d > c > 1.$$

故

$$\begin{aligned} n &= d^n - c^n = (d-c)(d^{n-1} + \cdots + dc^{n-2} + c^{n-1}) \\ &\geq d^{n-1} + \cdots + d + 1 \geq 3^{n-1} + \cdots + 3 + 1 > n. \end{aligned}$$

这是矛盾的,因而 $\left(\frac{m+n}{m}\right)^m$ 是无理数.

上述例题是一个综合运用知识的命题,解题过程中有三点具有示范作用:

1. 如何运用算术基本定理;
2. 如何运用等式中某些字母的互素关系去获得整除关系;
3. $d^n - c^n$ 的因式分解及应用.

这些方法和技巧,读者应予以重视.

最后,我们引入如下记号:若 $b^a \mid a$, 且 $b^{a+1} \nmid a$, 则称 b^a 恰整除 a , 记为 $b^a \parallel a$. 例如,我们有 $2^4 \parallel 2000, 5^3 \parallel 2000$. 将此记号运用于 a 的标准分解式(1.7), 就有

$$p_i^{a_i} \parallel a, \quad i = 1, 2, \dots, s.$$

练习题

1. 设 n 是正整数,试证方程 $x + y + 2xy = n$ 有正整数解的充要条件是 $2n + 1$ 为合数.
2. 试证有无限多个自然数 n , 使得 $6n \pm 1$ 同时是合数.
3. 试求所有的数 a , 使 $a, a + 4, a + 14$ 都是素数.
4. 设素数 $p \geq 5$, 且 $2p + 1$ 是素数, 试证 $4p + 1$ 必是合数.
5. 设 p_s 是全部由 1 构成的 s 位(十进制)整数, 试证若 p_s 是素数, 则 s 也是素数.
6. 设 $2^m + 1$ 是素数, 试证必有 $m = 2^n$, n 是非负整数.
7. 试证形如 $6m - 1$ 的素数有无限多个.
8. 设整数 a , 使得对任何自然数 n , 数 $n^4 + a$ 都是合数, 试证这样的 a 有无限多个.

§ 1.4 几个数论函数

对于任何正整数均有定义的函数,称为数论函数. 本节主要介绍高斯(Gauss)取整函数 $[x]$ 和它的性质. 此外,还介绍除数函数 $d(n)$ 和欧拉(Euler)函数 $\varphi(n)$ 的定义和

计算公式,为后面的讲解作准备.

一、函数 $[x]$

设 x 是实数,不大于 x 的最大整数称为 x 的整数部分,记为 $[x]$; $x - [x]$ 称为 x 的小数部分,记为 $\{x\}$. 例如, $[0.5] = 0$, $[\sqrt{50}] = 7$, $[-3] = -3$, $[-\pi] = -4$, $\{\pi\} = 0.1415\dots$, $\{-0.3\} = 0.7$ 等等.

由 $[x]$, $\{x\}$ 的定义可得到下列性质:

性质 1° $x - [x] = \{x\}$; $0 \leq \{x\} < 1$.

性质 2° $x - 1 < [x] \leq x < [x] + 1$.

性质 3° 设 $a \in \mathbf{Z}$, 则 $[a + x] = a + [x]$.

性质 4° $[x + y] \geq [x] + [y]$; $\{x + y\} \leq \{x\} + \{y\}$.

性质 5° $[-x] = \begin{cases} -[x], & x \in \mathbf{Z}; \\ -[x] - 1, & x \notin \mathbf{Z}. \end{cases}$

性质 6° 对于任意正整数 n , 有如下埃米特恒等式成立:

$$[x] + \left[x + \frac{1}{n}\right] + \left[x + \frac{2}{n}\right] + \dots + \left[x + \frac{n-1}{n}\right] = [nx].$$

性质 7° 若 $p^a \parallel n!$, 则

$$a = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \dots \quad (1.9)$$

注意(1.9)式虽写成有无限项的形式,但实际上对于固定的 n , 必存在正整数 s , 使 $p^s > n$, 因而 $0 < \frac{n}{p^s} < 1$, 故 $\left[\frac{n}{p^s}\right] = 0$. 而且, 当 $k > s$ 时, 都有 $\left[\frac{n}{p^k}\right] = 0$. 因此, (1.9)式实际上是有限项的和.

(1.9)式指出了阶乘数 $n!$ 的标准分解式中, 素因数 p 的指数 a 的计算方法.

【例 1.14】 试解方程 $\left[\frac{5+6x}{8}\right] = \frac{15x-7}{5}$.

【解】 因方程左边是整数, 因而右边的分式也是整数, 于是由性质 3° 知

$$\left[\frac{5+6x}{8} - \frac{15x-7}{5}\right] = -\frac{15x-7}{5} + \left[\frac{5+6x}{8}\right] = 0,$$

于是 $\left[\frac{81-90x}{40}\right] = 0$. 从而 $0 \leq \frac{81-90x}{40} < 1$, 故 $0 \leq 81-90x < 40$.

但 $\frac{15x-7}{5}$ 是整数, 故 $15x = 5t + 7, t \in \mathbf{Z}$. 代入前面所得的不等式, 得

$$0 \leq 39 - 30t < 40, \quad t \in \mathbf{Z}.$$

直接观察即知 $t = 0, 1$, 于是 $x = \frac{7}{15}, \frac{4}{5}$.

【例 1.15】 数 $100!$ 的十进位表示中, 末尾连续地有多少位全是零?

【解】 命题等价于 $100!$ 最多可被 10 的多少次方整除. 因 $10 = 2 \times 5$, 而由性质 7°

知 $100!$ 中 2 的指数大于 5 的指数, 所以 $100!$ 中 5 的指数就是所需求出的零的位数. 由

$$\alpha = \left[\frac{100}{5} \right] + \left[\frac{100}{5^2} \right] = 20 + 4 = 24,$$

即知 $100!$ 的末尾连续地有 24 位全是数码字 0.

二、函数 $d(n)$

正整数 n 的正因数的个数称为除数函数, 记为 $d(n)$. 由算术基本定理的推论 1 知, 若 n 的标准分解式为 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, 则利用乘法原理即可得到 $d(n)$ 的计算公式

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_s + 1).$$

三、欧拉函数 $\varphi(n)$

设 n 是正整数, $0, 1, \cdots, n-1$ 中与 n 互素的数的个数, 称之为 n 的欧拉函数, 记为 $\varphi(n)$. 若 n 的标准分解式是 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, 则 $\varphi(n)$ 计算公式是

$$\varphi(n) = p_1^{\alpha_1 - 1} p_2^{\alpha_2 - 1} \cdots p_s^{\alpha_s - 1} (p_1 - 1)(p_2 - 1) \cdots (p_s - 1).$$

例如,

$$\varphi(2000) = \varphi(2^4 5^3) = 2^3 5^2 (2-1)(5-1) = 800,$$

$$\varphi(2001) = \varphi(3 \cdot 23 \cdot 29) = (3-1)(23-1)(29-1) = 1432.$$

练习题

1. 试求方程 $\left[\frac{5+6x}{8} \right] = \frac{15x-7}{5}$ 的实数解 x .

2. 试求方程 $x^3 - [x] = 3$ 的实数解 x .

3. 对于任意实数 x, y , 试证

$$1) [2\{x\}] + [2\{y\}] \geq [\{x\} + \{y\}].$$

$$2) [2x] + [2y] \geq [x] + [x+y] + [y].$$

$$3) \left[\frac{nx}{n} \right] = [x].$$

4. 若 $\varphi(n) = 16$, 试找出至少 5 个 n 的值.

5. 试求出一个自然数 n , 满足 $\varphi(n) = 462000$.

6. 设 x 是任意实数, 试证

$$[x] + \left[x + \frac{1}{n} \right] + \left[x + \frac{2}{n} \right] + \cdots + \left[x + \frac{n-1}{n} \right] = [nx].$$

7. 设正整数 n 能被 $[\sqrt{n}]$ 整除, 试求 n .