数学奥林匹克小丛书

第三版

高中卷 15

Mathematical Olympiad Series

数　论

余红兵　著

华东师范大学出版社

总　序

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,既有扎实广泛的数学基础,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IMO获得奖牌的学生中,日后有不少成为大数学家.例如,获菲尔兹奖的数学家有:玛古利斯(G. Margulis,俄罗斯,1978年)、德里费尔德(V. Drinfeld,乌克兰,1990年)、约克兹(J. G. Yoccoz,法国,1994年)、博切尔兹(R. Borcherds,英国,1998年)、高尔斯(T. Gowers,英国,1998年)、拉福格(L. Lafforgue,法国,2002年)、佩雷尔曼(G. Perelman,俄罗斯,2006年)、陶哲轩(Terence Tao,澳大利亚,2006年)、吴宝珠(Bao Chau Ngo,越南,2010年)、林登施特劳斯(E. Lindenstrauss,以色列,2010年)、斯米尔诺夫(S. Smirnov,俄罗斯,2010年)、米尔扎哈尼(M. Mirzakhani,女,伊朗,2014年)、

阿维拉(A. Avila，巴西，2014 年)、舒尔茨(P. Scholze，德国，2018 年)、文卡特什(A. Venkatesh，澳大利亚，2018 年).

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，在数学竞赛活动中，应当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.

王元

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.

目　录

1 整　除

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、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 $|a| \geqslant |b|$. 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

$$a = bq + r，其中\ 0 \leqslant r < b，$$

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，…，$b-1$. 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 $\left[\frac{a}{b}\right]$(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：$0 \leqslant r < b$，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.

(5) 若 n 是正整数,则

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

(6) 若 n 是正奇数,则(在上式中用 $-y$ 代换 y)

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

例 1 证明:$1\underbrace{0\cdots0}_{200个0}1$ 被 1001 整除.

证明 由分解式(6),我们有

$$\begin{aligned}1\underbrace{0\cdots0}_{200个0}1 &= 10^{201} + 1 = (10^3)^{67} + 1 \\ &= (10^3+1)[(10^3)^{66} - (10^3)^{65} + \cdots - 10^3 + 1],\end{aligned}$$

所以,$10^3 + 1(=1001)$ 整除 $1\underbrace{0\cdots0}_{200个0}1$.

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

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

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

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 $n = a_k \times 10^k + \cdots + a_1 \times 10 + a_0$(这里 $0 \leqslant a_i \leqslant 9$,且 $a_k \neq 0$),则 $S(n) = a_0 + a_1 + \cdots + a_k$. 我们有

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

对 $1 \leqslant i \leqslant k$,由分解式(5)知 $9|(10^i-1)$,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 $9|(n-S(n))$. 由此易推出结论的两个方面.

注 1 整除性质(2)提供了证明 $b\mid(a_1+a_2+\cdots+a_n)$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：

$$b \text{ 整除每个 } a_i(i=1,2,\cdots,n).$$

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 $b\mid c_i$ $(i=1,2,\cdots,k)$. 读者将看到，为了证明 $b\mid a$，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 $k\geqslant 1$ 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 $n\geqslant 2$，记所说的和为 A，则

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

因 k 是正奇数，故由分解式(6)可知，对每个 $i\geqslant 2$，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 a, m, n 均是正整数，$a\geqslant 2$，证明：$a^m-1\mid a^n-1$ 的充分必要条件是 $m\mid n$.

证明 若 $m\mid n$，设 $n=mk$，则由(5)知 $a^m-1\mid a^n-1$.

反过来，设 $a^m-1\mid a^n-1$，作带余除法，设 $n=mk+r$，$0\leqslant r<m$，由

$$a^n-1=a^{mk+r}-1=(a^{mk}-1)a^r+(a^r-1),$$

及 $a^m-1 \mid a^n-1$ 可知，$a^m-1 \mid a^r-1$. 但 $0 \leqslant r < m$，故

$$0 \leqslant a^r-1 < a^m-1.$$

从而 $a^r-1=0$，(参见(3))结合 $a \geqslant 2$ 知必须 $r=0$，即 $m \mid n$.

带余除法，提供了间接证明 $b \mid a$ 的一个“平台”(与前面几个例子完全不同)：先作出等式 $a=bq+r$，其中 $0 \leqslant r < b$，再结合已知条件及其他信息，证明 $r=0$，从而 $b \mid a$.

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 $n \geqslant 2$，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 $K^n a_1 \cdots a_n$ 被任意两项的和 Ka_i+Ka_j 整除 $(1 \leqslant i, j \leqslant n, i \neq j)$. 由于 $n \geqslant 2$，显然，取

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

即符合要求(注意 Ka_1，…，Ka_n 互不相同).

例 8 设 n 是正整数，$n>1$，是否存在正整数，它被 $\underbrace{11\cdots1}_{n\text{个}}$ 整除，而且(十进制下的)各位数码之和小于 n?

解 记 $a_n=\underbrace{11\cdots1}_{n\text{个}}$. 设有符合要求的正整数，我们取 a 是其中的最小数. 由于 a_n，$2a_n$，…，$9a_n$ 的数码之和均不小于 n，故这些数均不是 a，从而 $a \geqslant 10a_n=10 \cdot \dfrac{10^n-1}{9}>10^n$.

设 a 的十进制表示为 $a=c_k \cdot 10^k+\cdots+c_1 \cdot 10+c_0$，其中 c_k，…，c_1，c_0 是数码，$0 \leqslant c_i \leqslant 9$，且 $c_k \neq 0$. 由于 $a>10^n$，故 $k \geqslant n$. 由于 $10^n-1=9a_n$，被 a_n 整除，故

$$b=a-(10^k-10^{k-n})=a-10^{k-n}(10^n-1) \quad ①$$

也被 a_n 整除，且 $0<b<a$.

另一方面，由①可知

$$b = c_k \cdot 10^k + \cdots + c_{k-n} \cdot 10^{k-n} + \cdots + c_1 \cdot 10 + c_0 - \underbrace{9\cdots9}_{n\text{个}}\underbrace{00\cdots0}_{k-n\text{个}}.$$

由此易知,若 $c_{k-n} < 9$,则 b 的数码之和等于 a 的数码之和,若 $c_{k-n} = 9$,则 b 的数码之和小于 a 的数码之和. 因此 b 的数码之和小于 n,且 b 被 a_n 整除,但 $0 < b < a$,这与 a 的最小值矛盾. 因此不存在符合要求的正整数.

习 题 1

1 设 n 和 k 都是正整数,则 $1, 2, \cdots, n$ 中恰有 $\left[\dfrac{n}{k}\right]$ 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 $n = \overline{a_k \cdots a_1 a_0}$ $(0 \leqslant a_i \leqslant 9,\ a_k \neq 0)$,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 $T(n)$.

4 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.

6 设 a、b 及 n 是给定正整数,若对任意正整数 $k(k \neq b)$,总有 $b-k \mid a-k^n$,证明:$a = b^n$.

7 设 m 是给定正整数,若有 n 个非负整数 $k_1, \cdots, k_n$,使得 $2^{k_1} + \cdots + 2^{k_n}$ 被 2^m-1 整除,则 $n \geqslant m$.

2 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±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±1),我们称 a 与 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 $a, b, \cdots, c$,可类似地定义它们的最大公约数 $(a, b, \cdots, c)$. 若 $(a, b, \cdots, c)=1$,则称 $a, b, \cdots, c$ 互素. 请注意,此时并不能推出 $a, b, \cdots, c$ 两两互素(即其中任意两个都互素);但反过来,若 $a, b, \cdots, c$ 两两互素,则显然有 $(a, b, \cdots, c)=1$.

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

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

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

$$ax+by=1.$$

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 $m|a$, $m|b$，则 $m|(a, b)$，即 a、b 的任一个公约数都是它们的最大公约数的约数.

(4) 若 $m>0$，则 $(ma, mb)=m(a, b)$.

(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 $(k\geqslant 2)$. 若 $(a, b)=1$，则 a、b 都是整数的 k 次幂. 一般地，设正整数 $a, b, \cdots, c$ 之积是一个整数的 k 次幂. 若 $a, b, \cdots, c$ 两两互素，则 $a, b, \cdots, c$ 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 $a, b, \cdots, c$，可类似地定义它们的最小公倍数 $[a, b, \cdots, c]$.

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 $a, b, \cdots, c$ 两两互素，则有

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

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

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.

例 1 对任意整数 n,证明分数$\dfrac{21n+4}{14n+3}$是既约分数.

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

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

因此所说的结论成立.

一般来说,互素整数 a、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 $d|r$ 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 记 $F_k=2^{2^k}+1$, $k\geqslant 0$. 证明:若 $m\neq n$,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 $d|2$,所以 $d=1$ 或 2.但 F_n 显然是奇数,故必须 $d=1$.

注 F_k $(k\geqslant 0)$ 称为费马(Fermat)数.例 2 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 3 的结论用处颇多,值得记住.

例 3 设 $a>1$, m, $n>0$,证明:

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

证明 设 $D=(a^m-1,\ a^n-1)$. 我们通过证明$(a^{(m,n)}-1)\mid D$及$D\mid(a^{(m,n)}-1)$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$(m,n)\mid m$，$(m,n)\mid n$，由第1单元中分解公式(5)即知$(a^{(m,n)}-1)\mid(a^m-1)$，以及$(a^{(m,n)}-1)\mid(a^n-1)$. 故由本单元的性质(3)可知，$a^{(m,n)}-1$整除$(a^m-1,\ a^n-1)$，即$(a^{(m,n)}-1)\mid D$.

为了证明$D\mid(a^{(m,n)}-1)$，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)

$$mu-nv=d. \tag{①}$$

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

$$D\mid a^{nv}(a^d-1). \tag{②}$$

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

综合已证得的两方面的结果，可知$D=a^{(m,n)}-1$.

例4 设a、b为正整数，则存在正整数u、v，使得$[a,b]=uv$，其中$u\mid a$，$v\mid b$，$(u,v)=1$.

证明 设$d=(a,b)$，$a=da_1$，$b=db_1$，其中$(a_1,b_1)=1$. 由(10)可知

$$[a,b]=da_1b_1.$$

由于d有正约数(例如1)与b_1互素，故d有最大的与b_1互素的约数，记为x，设$d=xy$.

我们证明，x与y互素. 因为设r是x、y的一个大于1的公约数，则由$r\mid x$知$(r,b_1)=1$，从而rx是d的一个与b_1互素的约数，但$rx>x$，这与x的选取矛盾. 故$(x,y)=1$.

进一步，因为(y,a_1)整除a_1，故它与b_1互素(因a_1与b_1互素)，因此可得$(y,a_1)=1$. 否则，$x\cdot(y,a_1)$是d的一个与b_1互素的约数，但它大于x，这与x的选取违背. 故$(y,a_1)=1$.

因此，$d=xy$，其中$(x,y)=1$，$(x,b_1)=1$，$(y,a_1)=1$.

记$u=a_1x$，$v=b_1y$，则$u\mid a$，$v\mid b$，又

$$(a_1,b_1)=(y,a_1)=(x,b_1)=(x,y)=1,$$

故$(u,v)=1$. 而$uv=a_1b_1xy=da_1b_1=[a,b]$.
这给出了$[a,b]$的符合要求的分解.

注 用下一单元讲的正整数的唯一分解定理,易给出本题一个更直接的证明.

例 5 设 $m, n > 0$, $mn \mid (m^2 + n^2)$, 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 $m_1 n_1 \mid (m_1^2 + n_1^2)$,故更有 $m_1 \mid (m_1^2 + n_1^2)$,从而 $m_1 \mid n_1^2$. 但 $(m_1, n_1) = 1$, 故 $(m_1, n_1^2) = 1$. 结合 $m_1 \mid n_1^2$,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 $m_1 n_1 \mid (m_1^2 + n_1^2)$ 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 $(d, c) = 1$.

现在,问题中的等式可化为

$$da_1 b_1 = ca_1 - cb_1, \qquad ①$$

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

设 $c = a_1 b_1 k$, 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 $k \mid d$. 从而 $k \mid (c, d)$(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.

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 $1+2+\cdots+n=\dfrac{n(n+1)}{2}$,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

$$\begin{aligned}&2(1^k+2^k+\cdots+n^k)\\ =&[1^k+(n-1)^k]+[2^k+(n-2)^k]+\cdots+[(n-1)^k+1^k]+2n^k\end{aligned}$$

是 n 的倍数. 同理,

$$2(1^k+2^k+\cdots+n^k)=[1^k+n^k]+[2^k+(n-1)^k]+\cdots+[n^k+1^k]$$

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 $b|a$,可将 b 分解为若干个两两互素的整数 b_1, b_2, $\cdots$, b_n 之积,而证明等价的 $b_i|a\ (i=1, 2, \cdots, n)$(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,请参考第 3 单元.

例 8 设整数 $a>b>1$,满足 $a+b \mid ab+1$, $a-b \mid ab-1$. 证明 $a<b\sqrt{3}$.

证明 由 $ab+1=(a+b)b-(b^2-1)$ 及 $a+b \mid ab+1$,可知 $a+b \mid b^2-1$.

同样,由 $ab-1=(a-b)b+b^2-1$,知 $a-b \mid b^2-1$. 故 b^2-1 是 $a+b$ 与 $a-b$ 的一个公倍数. 因此$[a+b, a-b] \mid b^2-1$. 因 $b^2-1>0$,故$[a+b, a-b] \leqslant b^2-1$. 即

$$\frac{(a+b)(a-b)}{(a+b, a-b)} \leqslant b^2-1. \quad ①$$

设 $d=(a+b, a-b)$,则 $d \mid a+b$, $d \mid a-b$,从而 d 整除$(a+b)+(a-b)=2a$,

同样 $d \mid 2b$. 故 $d \mid (2a, 2b)$，所以 $d \mid 2(a, b)$.

设 $d' = (a, b)$，则 $d' \mid a + b$, $d' \mid ab$，故由 $a + b \mid ab + 1$ 推出 $d' \mid 1$，故 $d' = 1$，而 $d \mid 2(a, b)$，故 $d \leqslant 2$. 因此由 ① 推出

$$\frac{(a+b)(a-b)}{2} \leqslant b^2 - 1,$$

故 $a^2 \leqslant 3b^2 - 2 < 3b^2$，因此 $a < b\sqrt{3}$.

习题 2

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：$(a^2 + b^2, ab) = 1$.

4 若一个有理数的 k 次幂是整数（$k \geqslant 1$），则这有理数必是整数. 更一般地，证明：一个首项系数为 ± 1 的整系数多项式的有理数根，必定是一个整数.

5 设 m、n、k 都是正整数，满足 $[m + k, m] = [n + k, n]$，证明：$m = n$.

6 设 a 是给定的正整数，d_n 为 $a + n^2$ 与 $a + (n+1)^2$ 的最大公约数（$n = 1, 2, \cdots$），求 d_n 的最大值.

7 设 $\{a_n\}$（$n \geqslant 1$）是一个正整数列. 若对任意 $i \neq j$，有 $(a_i, a_j) = (i, j)$. 则对任意 $i \geqslant 1$ 有 $a_i = i$.

3 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(称 n 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 p 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.

因此，两个整数互素的充分必要条件是：它们没有公共的素因子.

(2) 设 p 是素数，n 是任意一个整数，则或者 p 整除 n，或者 p 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 与 n 互素，或者 $p \mid n$.

素数的最为锐利的性质是下面的

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

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

由(3)特别地推出，若素数 p 整除 a^n $(n \geqslant 1)$，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 $p_1, p_2, \cdots, p_k$. 考虑数 $N=p_1 p_2 \cdots p_k+1$，显然 $N>1$，故 N 有素因子 p. 因 $p_1, p_2, \cdots, p_k$ 是全部素数，故 p 必等于某个 p_i $(1 \leqslant i \leqslant k)$，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 2 推出来:设 $F_k = 2^{2^k}+1\ (k \geqslant 0)$,则 $F_k > 1$,故 F_k 有素约数.因已证明无穷数列$\{F_k\}\ (k \geqslant 0)$ 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 $p_i\ (1 \leqslant i \leqslant k)$ 都是素数;并且,若 n 有两种素因数分解

$$n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l,$$

则必有 $k = l$,并且 $p_1, p_2, \cdots, p_k$ 是 $q_1, q_2, \cdots, q_l$ 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 $p_1, p_2, \cdots, p_k$ 是互不相同的素数,$\alpha_1, \alpha_2, \cdots, \alpha_k$ 是正整数,这称为 n 的标准分解.

由唯一分解定理不难得知:

设 a、b 为正整数,则 $b \mid a$ 的充分必要条件是:对每个素数 p,p 在 b 中出现的幂次不超过在 a 中出现的幂次;

设 $m>1$,则大于 1 的整数为一个 m 次方幂的充分必要条件是:m 的标准分解中,每个素数的幂次均被 m 整除.

(6) 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:

n 的全部正约数为 $p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$,其中 β_i 是满足 $0 \leqslant \beta_i \leqslant \alpha_i\ (i = 1, \cdots, k)$ 的任意整数.

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

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

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

由 $\tau(n)$的上述表示易知,n 为完全平方数的充分必要条件是 $\tau(n)$为奇数.这一结论,用处颇多.

(7) 若已知正整数 a、b 的标准分解,则易于给出(a, b)及$[a, b]$的表示:

设 $a = p_1^{\alpha_1}\cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1}\cdots p_k^{\beta_k}$, 这里 p_i 是素数,α_i、β_i 均是非负整数,不全为零. 则

$$(a, b) = p_1^{\gamma_1}\cdots p_k^{\gamma_k}\text{,其中 }\gamma_i = \min(\alpha_i, \beta_i),\ i = 1, \cdots, k.$$
$$[a, b] = p_1^{\delta_1}\cdots p_k^{\delta_k}\text{,其中 }\delta_i = \max(\alpha_i, \beta_i),\ i = 1, \cdots, k.$$

对于多于两个数的最大公约数及最小公倍数,有类似的结果.

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(8)中的结果相当有趣,它对任意 $n > 1$, 给出了 $n!$ 的标准分解.

(8) 对任意正整数 m 及素数 p,记号 $p^\alpha \parallel m$ 表示 $p^\alpha \mid m$, 但 $p^{\alpha+1} \nmid m$,即 p^α 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 $a_n = \underbrace{10001\cdots10001}_{n\text{个}1}$ $(n \geqslant 2)$, 则

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

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 为偶数时,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 $k \geqslant 2$, $\frac{10^{8k} - 1}{10^8 - 1}$也是大于 1 的整数. 故

$a_{2k}(k=2,3,\cdots)$ 都是合数. 又 $a_2=10\ 001=73\times137$ 是合数.

n 为奇数时,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 $n=2k+1$, $k\geqslant1$, 则

$$\begin{aligned}n^4+4^n&=n^4+4\cdot4^{2k}=n^4+4\cdot(2^k)^4\\&=n^4+4n^2\cdot(2^k)^2+4\cdot(2^k)^4-4n^2\cdot(2^k)^2\\&=(n^2+2\cdot2^{2k})^2-(2\cdot n\cdot2^k)^2\\&=(n^2+2^{k+1}n+2^{2k+1})(n^2-2^{k+1}n+2^{2k+1}).\end{aligned}$$

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 $k\geqslant1$), 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 $\dfrac{a}{c}=\dfrac{d}{b}=\dfrac{m}{n}$, 其中 m 和 n 是互素的正整数. 由 $\dfrac{a}{c}=\dfrac{m}{n}$ 意味着有理数$\dfrac{a}{c}$的分子、分母约去了某个正整数 u 后,得到既约分数$\dfrac{m}{n}$,因此

$$a=mu,\ c=nu. \tag{①}$$

同理,有正整数 v,使得

$$b = nv,\ d = mv. \qquad ②$$

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

$$(a+c)(a+d)=ap \qquad ③$$

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

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.

下面的例 4，是一个简单的结果，基于不同的考虑，可产生完全不同的证明.

例 4 设 a、b 为正整数，则 $\frac{(a+b)!}{a!b!}$ 是一个整数.

证法一 问题即为证明 $a!b!\mid(a+b)!$. 从数论角度看，这等价于证明，对每个素数 p，分母 $a!\ b!$ 中 p 的幂次，不超过分子 $(a+b)!$ 中 p 的幂次. 由(8)中的公式可知，这等价于证明

$$\sum_{l=1}^{\infty}\left[\frac{a+b}{p^l}\right]\geqslant\sum_{l=1}^{\infty}\left(\left[\frac{a}{p^l}\right]+\left[\frac{b}{p^l}\right]\right). \qquad ①$$

因此，只需证明 $\left[\frac{a+b}{p^l}\right]\geqslant\left[\frac{a}{p^l}\right]+\left[\frac{b}{p^l}\right]$. $(l=1,\ 2,\ \cdots)$

事实上，下面更一般的结果成立(与整数无关!)：

对任意实数 x、y，有

$$[x+y]\geqslant[x]+[y]. \qquad ②$$

为了证明②，我们注意，对任意整数 k 及任意实数 α，有 $[k+\alpha]=k+[\alpha]$. 由此可知，若 x 或 y 增加一个整数量，则②两边增加一个相同的量. 因此，只要对特殊情形 $0\leqslant x<1$，$0\leqslant y<1$ 证明②. 在此条件下，②的左边 $\geqslant 0$，右边为零，故②成立. 证毕.

证法二 注意到数列 $\{m!\}$ 的递推关系：$m!=m\cdot(m-1)!$，可对 $a+b$ 归纳，给出本题的一个代数证明.

易知 $a+b=2$ 时结论成立. 假设对所有满足 $a+b=n$ 的正整数 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

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

我们又有

$$(a+b)!=(a+b-1)!\cdot(a+b)=(a+b-1)!\cdot a+(a+b-1)!\cdot b. \tag{④}$$

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 $a!b!\mid(a+b)!$，即 $a+b=n+1$ 时结论也成立，这就完成了归纳证明.

证法三 考虑适当的计数模型，可导出本题的一个组合证明.

事实上，熟知 $\dfrac{(a+b)!}{a!b!}$ 是从 $a+b$ 个元素中，每次取 a 个的组合数 C_{a+b}^{a}，这当然是一个整数. 由此本题结论成立.

注 由例 4 的结果不难推出：对任意正整数 b，连续 b 个整数之积被 $b!$ 整除.

事实上，若这连续 b 个数均是正整数，设为 $a+1$，…，$a+b$，则 $\dfrac{(a+1)\cdots(a+b)}{b!}=\dfrac{(a+b)!}{a!b!}$ 是一个整数.

若连续 b 个整数均为负数，这显然化为前一种情形的结果.

若这连续 b 个整数中有正数有负数，则其中必有一个为零，结论显然成立.

例 5 设 m、n 是互素的正整数，证明：$m!n!\mid(m+n-1)!$.

证法一 与例 4 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”：

$$\left[\frac{m+n-1}{p^l}\right]\geqslant\left[\frac{m}{p^l}\right]+\left[\frac{n}{p^l}\right] \tag{②}$$

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 4 中②那样的对所有实数成立的结果来导出这里的②，我们需要利用所说整数的特别性质：

由带余除法，$m=p^lq_1+r_1$，$n=p^lq_2+r_2$，这里 $0\leqslant r_1$、$r_2<q^l$，而 q_1、q_2 均为非负整数，则有(参见第 1 单元的(4))

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

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

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

这就证明了②. 证毕.

证法二 由例 4 可知，$\dfrac{(m+n-1)!}{m!(n-1)!}$ 与 $\dfrac{(m+n-1)!}{(m-1)!n!}$ 均是整数. 因此，若设 $A=\dfrac{(m+n-1)!}{m!n!}$，则 mA 与 nA 均是整数，故 $mnA=m\cdot nA$ 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.

或者，换一种表述：

由于 $(m, n)=1$，故存在整数 x、y，使得

$$mx+ny=1.$$

两边乘以 $\dfrac{(m+n-1)!}{m!n!}$，得

$$\frac{(m+n-1)!}{(m-1)!n!}x+\frac{(m+n-1)!}{m!(n-1)!}y=\frac{(m+n-1)!}{m!n!}.$$

上式左边为整数，故右边也是整数. 证毕.

例 6 设 a、b、n 均为正整数，$a^n \mid b$，证明：$(a+1)^b-1$ 被 a^{n+1} 整除.

证法一 由二项式定理得

$$(a+1)^b-1=\sum_{k=1}^{b}\mathrm{C}_b^k a^k.$$

我们将证明，a^{n+1} 整除 $C_b^k a^k (k=1,\cdots,b)$，由此及上式即证明了本题结论.

注意 $a^k C_b^k = a^k \cdot \frac{b}{k} C_{b-1}^{k-1}$. 设 p 是 a 的任一个素因子，并设 $p^\alpha \parallel a$. 由于 $a^n \mid b$，故 b 中 p 的幂次至少是 $n\alpha$，又因 $p \geqslant 2$，故 $k \leqslant p^{k-1}$，故 p 在 k 中的幂次 $\leqslant k-1$. 因此 p 在 $a^k \cdot \frac{b}{k}$ 中的幂次 $\geqslant k\alpha + n\alpha - (k-1) \geqslant (k+n)\alpha - (k-1)\alpha = (n+1)\alpha$. 故 $p^{(n+1)\alpha} \mid a^k C_b^k$. 又 p 在 a^{n+1} 中的幂次为 $(n+1)\alpha$. 因此 $a^{n+1} \mid a^k C_b^k$，对 $k=1,\cdots,b$ 均成立. 证毕.

证法二 注意到数列 $\{a^n\}$ 满足递推关系：$a^{n+1} = a \cdot a^n$，我们可对 n 归纳，导出本题的一个代数证明.

当 $n=1$ 时，设 $b=aq$，由

$$(a+1)^b - 1 = (a+1)^{aq} - 1 = a^{aq} + aq \cdot a^{aq-1} + \cdots + aq \cdot a$$

可见，上式右边每一项均是 a^2 的倍数，故 a^2 整除左边.

设 $n=k$ 时结论成立.

当 $n=k+1$ 时，设 $a^{k+1} \mid b'$.

记 $b = \frac{b'}{a}$，则 $a^k \mid b$. 我们有

$$\begin{aligned}(a+1)^{b'} - 1 &= [(a+1)^b]^a - 1 \\ &= [(a+1)^b - 1][(a+1)^{(a-1)b} + \cdots + (a+1)^b + 1].\end{aligned}$$

由归纳假设知，上式右边第一项被 a^{k+1} 整除，而第二个括号内共有 a 项，将每项展开后，具有形式 $Aa + \underbrace{1+\cdots+1}_{a\text{个}} = Aa + a$（其中 A 是一个整数），故被 a 整除，因此 $a^{k+2} \mid [(a+1)^{b'} - 1]$. 即 $n=k+1$ 时结论也成立. 证毕.

例 7 (1) 证明：对任意正整数 n，存在正整数构成的 n 元集合 S，使得对任意 $k\ (1 \leqslant k \leqslant n)$，$S$ 中任意 k 元子集中的元素之积，是一个 k 次方幂；

(2) 证明：不存在正整数构成的无穷集合 S，使得对任意正整数 k，S 中任意 k 元子集中的元素之积，均是 k 次方幂.

证明 (1) 可任取 n 个互不相同的正整数 $a_1,\cdots,a_n$. 令 $b_i = a_i^{n!}\ (i=1,\cdots,n)$. 这 $b_1,\cdots,b_n$ 中任意 k 个的积，是一个 $n!$ 次幂，因为 $k \mid n!\ (1 \leqslant k \leqslant n)$，故是一个 k 次幂.

(2) 假设有符合问题要求的无穷集合 S. 任取 $a, b \in S$，$a \neq b$. 则有一个素数 p，使 p 在 a 中出现的幂次 α，与 p 在 b 中出现的幂次 β 不相同.

对任意整数 $k \geqslant 2$，在 S 中再任取 $k-1$ 个元素 $n_1,\cdots,n_{k-1}$. 设 p 在 n_i 中的幂次为 x_i，则由于 $a \cdot n_1 \cdots n_{k-1}$，$b \cdot n_1 \cdots n_{k-1}$ 均是整数的 k 次方，故特别地，

$$\alpha + x_1 + \cdots + x_{k-1}, \beta + x_1 + \cdots + x_{k-1}$$

均是 k 的倍数(参见前面的(5)),从而它们的差被 k 整除,即 $k \mid \alpha - \beta$. 但 k 是任意正整数,故必须 $\alpha - \beta = 0$, 即 $\alpha = \beta$. 这与前面说的 $\alpha \neq \beta$ 相违. 故所说的 S 不存在.

习 题 3

1 证明:对任意给定的正整数 $n > 1$, 都存在连续 n 个合数.

2 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.

5 设 $n > 1$ 为整数,$S_n = \{x \in \mathbf{N} \mid (x, n) \neq 1\}$. 求所有 n,具有性质:若 x, $y \in S_n$,则 $x + y \in S_n$.

6 设 $f(x)$是一个非常数的整系数多项式,证明:数列 $\{|f(n)|\}(n \geqslant 1)$ 中包含无穷多个素因子.

4 不定方程（一）

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

$$(z-y)(z+y)=2^2\times 17. \qquad ①$$

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

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

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.

解 关键的一步(也是本题的主要困难)是看出方程可分解为

$$(x+y+z)(x+y-z)(y+z-x)(z+x-y)=-2^3\times 3.\qquad ①$$

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 2^4 整除,但①的右边不是 2^4 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:对①先模 2,然后再模 2^4.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

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

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(见第 2 单元中的(8)),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 $k\geqslant 2$).

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

$$(y-x)(y+x+1)=x^3. \qquad ①$$

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 $p\mid x^3$,故素数 p 整除 x,结合 $p\mid(y-x)$ 知 $p\mid y$,但 $p\mid(x+y+1)$,从而 $p\mid 1$,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

$$b^3-a^3=2ab+1. \qquad ②$$

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

$$(b-a)(b^2+ab+a^2)=2ab+1. \qquad ③$$

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 $x\geqslant 1$.

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，$k\geqslant 2$，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 $x\geqslant 2$ 及 y，使得

$$(x-1)x(x+1)=y^k. \qquad ①$$

请注意上面左端的三个因数 $x-1$、x、$x+1$ 并非总是两两互素，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

$$(x^2-1)x=y^k. \qquad ②$$

因正整数 x 和 x^2-1 互素，故由②推出，有正整数 a、b，使得

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

由此我们有

$$\begin{aligned}1&=a^{2k}-b^k=(a^2)^k-b^k\\&=(a^2-b)(a^{2k-2}+a^{2k-4}b+\cdots+a^2b^{k-2}+b^{k-1}),\end{aligned}$$

由于 $x\geqslant 2$，故 $a\geqslant 2$，又 $k\geqslant 2$，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、y 为整数，故 $|x|\geqslant y+1$，或 $|x|\leqslant y-1$.

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

当 $|x|\leqslant y-1$ 时，此时 $y-1\geqslant 0$，且

$$y^2-x^2\geqslant y^2-(y-1)^2=2y-1>0,$$

故方程左边 $\geqslant(2y-1)^2$.

因此由原方程产生

$$(2y-1)^2 \leqslant 1+16y,$$

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

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

证明 首先，将 $(x+1)^{x+1}$ 展开即知

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

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

$$y^y + z^z > y^y \geqslant (x+1)^y \geqslant (x+1)^{x+1} > 2x^x (\text{由 ①}),$$

产生矛盾.

因此 $y \leqslant x$，$z \leqslant x$，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 $x \geqslant 1$.

例 8 设 m 是给定正整数，求所有正整数 n、x、y，满足 m、n 互素，且

$$(x^2+y^2)^m = (xy)^n.$$

解 设 n、x、y 是方程的一组正整数解，由

$$(xy)^n = (x^2+y^2)^m \geqslant (2xy)^m$$

可知 $n > m$.

我们证明必有 $x = y$. 为此，设 p 是任一个素数，p 在 x，y 中出现的幂次分别是 α 及 β，我们只要证明 $\alpha = \beta$.

事实上，p 在 $(xy)^n$ 中出现的幂次为 $(\alpha+\beta)n$；若 $\alpha \neq \beta$，可设 $\alpha < \beta$，则 p 在 $(x^2+y^2)^m$ 中出现的幂次为 $2\alpha m$. 故 $2\alpha m = (\alpha+\beta)n$. 但 $n > m$，故

$$\begin{aligned}(\alpha+\beta)n &= \alpha n + \beta n \\ &> \alpha m + \alpha m = 2\alpha m,\end{aligned}$$

矛盾. 故 $\alpha = \beta$，从而 $x = y$. 故方程化为 $(2x^2)^m = x^{2n}$，即 $x^{2(n-m)} = 2^m$，因此 x

图书在版编目(CIP)数据

数论/余红兵著.—3 版.—上海:华东师范大学出版社,2019
(数学奥林匹克小丛书.高中卷)
ISBN 978-7-5675-9501-9

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(2019)第 242174 号

数学奥林匹克小丛书(第三版)·高中卷
数论(第三版)

著　　者　余红兵
总 策 划　倪　明
责任编辑　孔令志
特约审读　徐惟简
责任校对　时东明
装帧设计　高　山
责任发行　颜星华

出版发行　华东师范大学出版社
社　　址　上海市中山北路 3663 号　邮编 200062
网　　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
地　　址　上海市中山北路 3663 号华东师范大学校内先锋路口
网　　店　http://hdsdcbs.tmall.com

印 刷 者　山东韵杰文化科技有限公司
开　　本　787×1092　16 开
插　　页　1
印　　张　6.75
字　　数　112 千字
版　　次　2020 年 4 月第三版
印　　次　2020 年 4 月第一次
印　　数　1—30 100
书　　号　ISBN 978-7-5675-9501-9
定　　价　22.00 元

出 版 人　王　焰

华东师大社主办的 QQ 群（部分）：

1. 华师—小学奥数教练 2 群，群号：689181206
2. 华师—初中数学教师 2 群，群号：112892422
3. 华师—中学奥数教练群，群号：545921244
4. 华师—高中数学教师群，群号：319118349
5. 华师—初中理科学生群，群号：609160454
6. 华师—高中理科学生群，群号：455685245

欢迎广大师生加入相应的群中。