数学奥林匹克小丛书 高中卷 12

Shuxue Aolinpike

XIAOCONG SHU

数学竞赛中的 数论问题

余红兵 著

华东师范大学出版社

olinpike

数学奥林匹克小丛书

高中卷 12

数学竞赛中的数论问题

linpike Xiao Congshu ● 余红兵 著

77/80

华东师范大学出版社

图书在版编目（CIP）数据

数学奥林匹克小丛书．高中卷．数学竞赛中的数论问题／余红兵著．—上海：华东师范大学出版社，2005.3
ISBN 7-5617-4161-8

I.数... II.余... III.数学课-高中-教学参考资料 IV.G634.603

中国版本图书馆CIP数据核字(2005)第019481号

数学奥林匹克小丛书·高中卷
数学竞赛中的数论问题

著　　者　余红兵
策划组稿　倪　明
责任编辑　审校部编辑工作组
特约编辑　余海峰
封面设计　高　山
版式设计　蒋　克

出版发行　华东师范大学出版社
　　　　　市场部 电话 021-62865537
　　　　　门市(邮购) 电话 021-62869887
　　　　　门市地址 华东师大校内先锋路口
业务电话　上海地区 021-62232873
　　　　　华东 中南地区 021-62458734
　　　　　华北 东北地区 021-62571961
　　　　　西南 西北地区 021-62232893
业务传真　021-62860410 62602316
http://www.ecnupress.com.cn
社　　址　上海市中山北路3663号
　　　　　邮编 200062

印 刷 者　江苏句容市排印厂
开　　本　787x960 16开
印　　张　5.5
字　　数　88千字
版　　次　2005年4月第一版
印　　次　2005年4月第一次
印　　数　11 000
书　　号　ISBN 7-5617-4161-8/G·2386
定　　价　8.00元

出 版 人　朱杰人

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 $b \mid a$，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 $b \mid c$，且 $c \mid a$，则 $b \mid a$，即整除性质具有传递性.

(2) 若 $b \mid a$，且 $b \mid c$，则 $b \mid (a \pm c)$，即为某一整数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 $b \mid a$ 及 $b \mid c$，则对任意整数 u、v 有 $b \mid (au + cv)$. 更一般地，若 $a_1, a_2, \cdots, a_n$ 都是 b 的倍数，则 $b \mid (a_1 + a_2 + \cdots + a_n)$.

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

$$a = bq + r, \text{其中 } 0 \leqslant r < b,$$

并且 q 和 r 由上述条件惟一确定.

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：$0, 1, \cdots, b-1$. 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 $\left[\frac{a}{b}\right]$ $\left(\text{不超过}\frac{a}{b}\text{的最大整数}\right)$，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 $b \mid a$ 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 1 001 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, $10^3+1(=1\ 001)$ 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 $b\mid a$ 不易入手,我们可以尝试着选择适当的"中间量"c,来证明 $b\mid c$ 及 $c\mid a$, 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: $9\mid n$ 的充分必要条件是 $9\mid S(n)$.

证明 设 $n=a_k\times10^k+\cdots+a_1\times10+a_0$ (这里 $0\leqslant a_i\leqslant9$,且 $a_k\neq0$),则 $S(n)=a_0+a_1+\cdots+a_k$. 我们有

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

对 $1 \leqslant i \leqslant k$，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.

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”，这是数论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 $n \leqslant m$ 时，易知结论成立. 事实上，$m = n$ 时，结论平凡；$n < m$ 时，结果可由 $2^n + 1 \leqslant 2^{m-1} + 1 < 2^m - 1$ 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，$n = mq + r$，$0 \leqslant r < m$，而 $q > 0$. 由于

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

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

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.

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.

(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

$$ax + by = 1,$$

这通常称为 a、b 适合的裴蜀等式.

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 $d \mid a$ 且 $d \mid b$，故 $d \mid ax$ 及 $d \mid by$，于是 $d \mid (ax + by)$，即 $d \mid 1$，从而 $d = 1$.

由(1)及(2)不难导出下面的几个基本结论：

(3) 若 $m \mid a$，$m \mid b$，则 $m \mid (a, b)$，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 $b \mid ac$. 若 $(b, c) = 1$，则 $b \mid a$.

(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 $a \mid d, b \mid d, \cdots, c \mid d$, 且 $a, b, \cdots, c$ 两两互素,则有 $ab\cdots c \mid d$.

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),下面几个例子体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 $d \mid r$. 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 $a \mid (by-r)$ 或 $b \mid (ax-r)$, 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

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

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 $F_k=2^{2^k}+1$, $k \geqslant 0$. 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 $d\mid 2$，所以 $d=1$ 或 2. 但 F_n 显然是奇数,故必须 $d=1$.

注 $F_k(k\geqslant 0)$ 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:

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

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(参见本单元性质(1)中的注释)

$$mu-nv=d. \qquad ①$$

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

$$D\mid a^{nv}(a^d-1). \qquad ②$$

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

证明 设 $(m,\ n)=d$，则 $m=m_1d$, $n=n_1d$, 其中 $(m_1,\ n_1)=1$.

于是,已知条件化为 $m_1n_1\mid(m_1^2+n_1^2)$，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 $m_1 n_1 \mid (m_1^2 + n_1^2)$ 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 $b_1 \mid c$. 再由 $(a_1, b_1) = 1$ 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(习题 3 第 5 题).

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

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

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 $b \mid a$ 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 $b \mid a$ 分解为等价的两个命题 $b_1 \mid a$ 及 $b_2 \mid a$,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 $a_1b_1 \mid c$ 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,$\cdots$,b_n 之积,而证明等价的 $b_i \mid a$ $(i=1, 2, \cdots, n)$(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 5.

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:$m=n$.

3 素数及惟一分解定理

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.

(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 3 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,即正整数的惟一分解定理,或算术基本定理,它表现了素数在正整数集合中的真正分量.

(5)(惟一分解定理) 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,这样的分解是惟一的.

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 可惟一地表示为

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

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.

若已知正整数 n 的(如上所述的)标准分解,则由惟一分解定理,可确定其全部的正约数:

(6) 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,若证 $\tau(n)$ 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 $p^\alpha \parallel m$ 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 $a_n=\underbrace{10\,001\cdots 10\,001}_{n\text{个}1}(n\geqslant 2)$, 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. 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 $a_2=10\,001=13\times 137$ 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 $n=2k+1$, $k\geqslant 1$, 则