# CyanMath: 创美营讲义（数学）

LeyuDame

2024 年 10 月 30 日

# 目录

# 符号说明

| 符号 | 说明 |
|---|---|
| $a \mid b$ | $a$ 整除 $b$ |
| $a \nmid b$ | $a$ 不整除 $b$ |
| $(a,b)$ | $a$ 与 $b$ 的最大公因数 |
| $[a,b]$ | $a$ 与 $b$ 的最小公倍数 |
| $p^\alpha \| a$ | $p^\alpha \mid a$ 但 $p^{\alpha+1} \nmid a$ |
| $a \equiv b(\bmod m)$ | $a$ 与 $b$ 对模 $m$ 同余 |
| $a \not\equiv b(\bmod m)$ | $a$ 与 $b$ 对模 $m$ 不同余 |
| $a^{-1}(\bmod m)$ | $a$ 对模 $m$ 的数论倒数 |
| $[x]$ | 不超过 $x$ 的最大整数 |
| $\max\{a,b\}$ | 实数 $a$ $b$ 中较大的数 |
| $\min\{a,b\}$ | 实数 $a$ $b$ 中较小的数 |

表 1: 符号说明

# 第一章　整除, 同余和不定方程

## 1.1　整除

任意两个整数的和, 差或积都是整数, 但是两个整数做除法时所得的结果不一定是整数, 因此, 数论中的许多问题都是在研究整数之间的除法.

### 1.1.1　整除的概念与基本性质

**定义 1.1.1.** 对任给的两个整数 $a, b(a \neq 0)$, 如果存在整数 $q$, 使得 $b = aq$, 那么称 $b$ 能被 $a$ 整除 (或称 $a$ 能整除 $b$ ), 记作 $a \mid b$. 否则, 称 $b$ 不能被 $a$ 整除, 记作 $a \nmid b$ .

如果 $a \mid b$, 那么称 $a$ 为 $b$ 的因数, $b$ 为 $a$ 的倍数.

利用整除的定义，可以非常容易地推导出下面一些经常被用到的性质.

**性质 1.1.1.** 如果 $a \mid b$, 那么 $a \mid (-b)$ ，反过来也成立; 进一步, 如果 $a \mid b$, 那么 $(-a) \mid b$ ，反过来也成立.

因此, 我们经常只讨论正整数之间的整除关系.

**性质 1.1.2.** 如果 $a|b, b|c$, 那么 $a \mid c$ . 这表明整除具有传递性.

**性质 1.1.3.** 若 $a|b, a|c$, 则对任意整数 $x, y$, 都有 $a \mid bx + cy$ . (即 $a$ 能整除 $b, c$ 的任意一个“线性组合”)

**例 1.1.1.** 若 $a|n, b|n$, 且存在整数 $x, y$, 使得 $ax + by = 1$, 证明: $ab \mid n$.

**证明.** 由条件, 可设 $n = au, n = bv, u, v$ 为整数. 于是

$$\begin{aligned} n &= n(ax+by) \\ &= nax+nby \\ &= abvx+abuy \\ &= ab(vx+uy) \end{aligned}$$

因此

$$ab \mid n$$

□

**注记.** *一般地, 由 $a|n, b|n$, 并不能推出 $ab \mid n$, 例如 $2|6, 6|6$, 但 $12 \nmid 6$. 题中给出的条件实质上表明 $a, b$ 的最大公因数 (见 1.3 节) 为 1 , 即 $a$ 与 $b$ 互素，在此条件下可推出 $ab \mid n$ .*

**例 1.1.2.** 证明：无论在数 12008 的两个 0 之间添加多少个 3 ，所得的数都是 19 的倍数.

**证明.** 记 $a_0 = 12008, a_n = 120\underbrace{3\cdots 3}_{n\uparrow 3}08, n = 1, 2, \cdots$.

首先，因为

$$a_0 = 19 \times 632$$

故

$$19 \mid a_0$$

其次，设 $19 \mid a_n$ ，则由

$$a_{n+1} - 10a_n = 228 = 19 \times 12$$

可知

$$19 \mid a_{n+1}.$$

所以，对一切整数 $n$ ，数 $a_n$ 都是 19 的倍数. □

**注记.** *此题的处理过程中运用了递推的思想，其基本思路是将 $a_{n+1}$ 表示为 $a_n$ 与 19 的一个线性组合.*

**例 1.1.3.** 已知一个 1000 位正整数的任意连续 10 个数码形成的 10 位数是 $2^{10}$ 的倍数. 证明：该正整数为 $2^{1000}$ 的倍数.

**证明.** 设该正整数 $x=\overline{a_1a_2\cdots a_{1000}}$, 其中 $a_i$ 是十进位数码. 由条件, 可知

$$2^{10}\ |\overline{a_{991}\cdots a_{1000}},2^{10}\mid\overline{a_{990}\cdots a_{999}},\tag{1.1}$$

因此

$$2^{10}\mid\overline{a_{990}\cdots a_{999}}\times 10.\tag{1.2}$$

记 $y=\overline{a_{991}\cdots a_{999}}$ ，则式 1.2又可写作

$$2^{10}\mid a_{990}\times 10^{10}+10y,$$

故

$$2^{10}\mid 10y.$$

结合 $2^{10}\mid\overline{a_{991}\cdots a_{1000}}$ ，可知

$$2^{10}\mid 10y+a_{1000},$$

于是

$$2^{10}\mid a_{1000},$$

这要求

$$a_{1000}=0.$$

类似地，朝前倒推，可得

$$a_{11}=\cdots=a_{1000}=0,$$

即

$$x=\overline{a_1\cdots a_{10}}\times 10^{990}.$$

再结合条件 $2^{10}\mid\overline{a_1\cdots a_{10}}$ ，即可得

$$2^{1000}\mid x.$$

□

**注记.** 这里先证明 $a_{11}=\cdots=a_{1000}=0$ 是非常关键的，在证明中利用 $\overline{a_{991}\cdots a_{999}}$ 来过渡也是比较巧妙的.

例 4 设 $m$ 是一个大于 2 的正整数，证明：对任意正整数 $n$ ，都有 $2^m-1\nmid 2^n+1$.

证明如果存在正整数 $n$, 使得 $2^m-1\mid 2^n+1$ ，那么取其中最小的那个 $n$ .

由于 $m>2$, 知 $n>1$, 进一步, 应有 $2^n+1\geqslant 2^m-1$, 知 $n\geqslant m$ ，而 $n=m$ 时，将导致 $2^m-1\mid 2$ （因为 $2=(2^n+1)-(2^n-1)$ ，右边每一项都是 $2^n-1$ 的倍数)，矛盾，故 $n>m$ .

现在，设 $2^n+1=(2^m-1)\,q$ ，这里 $q$ 为正整数，则

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

即

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

于是，

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

得 $2^{n-m}+1=(2^m-1)\left(q-2^{n-m}\right)$ ，因此，$2^m-1\mid 2^{n-m}+1$ ，与 $n$ 的最小性矛盾.

所以，命题成立.

说明这里用到了两个结论：一个是” 若 $a\mid b, b\neq 0$ ，则 $|a|\leqslant|b|$” ，它由整除的定义可直接证出. 另一个是” 任意多个正整数中必有最小元”，这是著名的” 最小数原理”.

### 1.1.2　素数与合数

对任意正整数 $n>1$, 如果除 1 与 $n$ 以外，$n$ 没有其他的因数，那么称 $n$ 为素数. 否则称 $n$ 为合数. 这样，我们将正整数分为了三类：1 ，素数，合数.

素数从小到大依次为 $2,3,5,7,11,\cdots$ . 我们可以非常轻松地写出 100 以内的所有素数，共 25 个. 但是并不是对每个素数 $p$ ，都能轻易地指出 $p$ 后面的一个素数是多少. 事实上，当 $p$ 比较大时，求出它后面的那个素数是十分困难的. 正是素数的这种无规律性，初等数论才显得魅力无穷, 具有很强的挑战

性和极大的吸引力.

素数与合数具有如下的一些性质.

性质 1 设 $n$ 为大于 1 的正整数, $p$ 是 $n$ 的大于 1 的因数中最小的正整数, 则 $p$ 为素数.

性质 2 如果对任意 1 到 $\sqrt{n}$ 之间的素数 $p$, 都有 $p \nmid n$, 那么 $n$ 为素数. 这里 $n(>1)$ 为正整数.

证明事实上, 若 $n$ 为合数, 则可写 $n=pq, 2 \leqslant p \leqslant q$. 因此 $p^2 \leqslant n$, 即 $p \leqslant \sqrt{n}$ .

这表明 $p$ 的素因子 $\leqslant \sqrt{n}$ ，且它是 $n$ 的因数，与条件矛盾. 因此 $n$ 为素数.

说明这里素因子是指正整数的因数中为素数的那些数, 此性质是我们检验一个数是否为素数的最常用的方法.

性质 3 素数有无穷多个.

证明若只有有限个素数, 设它们是 $p_1<p_2<\cdots<p_n$. 考虑数

$$x=p_1 p_2 \cdots p_n+1$$

其最小的大于 1 的因数 $p$, 它是一个素数, 因此, $p$ 应为 $p_1, p_2, \cdots, p_n$ 中的某个数. 设 $p=p_i, 1 \leqslant i \leqslant n$, 并且 $x=p_i y$, 则 $p_1 p_2 \cdots p_n+1=p_i y$, 即 $p_i(y-\ p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_n)=1$. 这导致 $p_i \mid 1$. 矛盾.

所以, 素数有无穷多个.

说明如果将所有的素数从小到大依次写出为 $2=p_1<p_2<\cdots$, 并写 $q_n=p_1 p_2 \cdots p_n+1$, 那么

$$q_1=3, q_2=7, q_3=31, q_4=211, q_5=2311$$

它们都是素数. 是否每一个 $n$ 都有 $q_n$ 为素数呢? 我们不能被表面现象所迷惑, 再朝下算, 可知 $q_6=59 \times 509$ 就是一个合数. 事实上, 后面的 $q_7, q_8, q_9$, $q_{10}$ 都是合数. 到目前为止, 人们还不知道数列 $q_1, q_2, \cdots$ 中是否有无穷多个素数, 也不知道其中是否有无穷多个合数.

性质 4 素数中只有一个数是偶数，它是 2 .

例 1 设 $n$ 为大于 1 的正整数. 证明: 数 $n^5+n^4+1$ 不是素数.

证明注意到

$$\begin{aligned}
& n^5+n^4+1 && (1.3)\\
= & n^5+n^4+n^3-\left(n^3-1\right) && (1.4)\\
= & n^3\left(n^2+n+1\right)-(n-1)\left(n^2+n+1\right) && (1.5)\\
= & \left(n^3-n+1\right)\left(n^2+n+1\right) && (1.6)
\end{aligned}$$

因此, 若 $n^5+n^4+1$ 为素数, 则 $n^3-n+1=1$, 这要求 $n=0$ 或 $\pm1$ .
故当 $n>1$ 时，$n^5+n^4+1$ 不是素数.
说明利用因式分解来判断一个数是否为素数是数论中的常见方法，后面也将不断用到.

例 2 考察下面的数列:

$$101, 10101, 1010101, \cdots$$

问: 该数列中有多少个素数?
解易知 101 是素数. 下证这是该数列中仅有的一个素数.

$$\text{记} a_n=\underbrace{10101\cdots01}_{n\text{ 个}01}, \text{则当} n\geqslant 2 \text{ 时, 有} \tag{1.7}$$

$$a_n=10^{2n}+10^{2(n-1)}+\cdots+1 \tag{1.8}$$

$$=\frac{10^{2(n+1)}-1}{10^2-1} \tag{1.9}$$

$$=\frac{\left(10^{n+1}-1\right)\left(10^{n+1}+1\right)}{99}. \tag{1.10}$$

注意到，$99<10^{n+1}-1, 99<10^{n+1}+1$ ，而 $a_n$ 为正整数，故 $a_n$ 是一个合数（因为分子中的项 $10^{n+1}-1$ 与 $10^{n+1}+1$ 都不能被 99 约为 1 ).

说明这里需要将因式分解式 $x^n-1=(x-1)\left(x^{n-1}+x^{n-2}+\cdots+1\right)$ 反用，高中阶段它被作为等比数列求和的公式.

例 3 求所有的正整数 $n$, 使得 $\frac{n(n+1)}{2}-1$ 是一个素数.
解记 $a_n=\frac{n(n+1)}{2}-1$ ，则 $a_1=0$ 不是素数，因此只需讨论 $n>1$ 的情形. 我们利用 $n$ 只能是形如 $4k, 4k+1, 4k+2, 4k+3$ 的数分别讨论.

当 $n$ 是形如 $4k+2$ 或 $4k+1$ 的数时, $a_n$ 都是偶数, 要 $a_n$ 为素数, 只能是

$$\frac{n(n+1)}{2}-1=2$$
$$n=2$$

解得
当 $n=4k$ 时，可得

$$a_n = 2k(4k+1) - 1 \tag{1.11}$$
$$= 8k^2 + 2k - 1 \tag{1.12}$$
$$= (4k-1)(2k+1), \tag{1.13}$$

这是一个合数.
当 $n = 4k+3$ 时, 可得

$$a_n = 2(k+1)(4k+3) - 1 \tag{1.14}$$
$$= 8k^2 + 14k + 5 \tag{1.15}$$
$$= (4k+5)(2k+1), \tag{1.16}$$

仅当 $k = 0$ ，即 $n = 3$ 时，$a_n$ 为素数.
所以，满足条件的 $n = 2$ 或 3.
说明对 $n$ 分类处理一方面是去分母的需要，另一方面是为进行因式分解做准备.

例 4 对任意正整数 $n$ ，证明：存在连续 $n$ 个正整数，它们都是合数.
证明设 $n$ 为正整数，则

$$(n+1)! + 2, (n+1)! + 3, \cdots, (n+1)! + (n+1)$$

是 $n$ 个连续正整数, 并且第 $k$ 个数是 $k+1$ 的倍数（且大于 $k+1$ ），故它们是连续的 $n$ 个合数.

说明这个结论表明：对任意正整数 $n$ ，都存在两个素数，它们之间至少有 $n$ 个数，且这些数都是合数. 但是，让我们来看一些素数对（3，5），（5，7），
（11，13），（17，19），…，（1997，1999），它们所含的两个素数都只相差 2（这是两个奇素数的最小差距），这样的素数对称为孪生素数. 是否存在无穷多对素数，它们是孪生素数？这是数论中一个未解决的著名问题.

例 5 设 $n$ 为大于 2 的正整数. 证明：存在一个素数 $p$ ，满足 $n < p < n!$ .
证明设 $p_1 < p_2 < \cdots < p_k$ 且 $p_1, p_2, \cdots, p_k$ 是所有不超过 $n$ 的素数，考虑数

$$q = p_1 p_2 \cdots p_k - 1$$

在 $n>2$ 时，2,3 都在 $p_1,\cdots,p_k$ 中出现，故 $5\leqslant q\leqslant n!-1<n!$ ，利用性质 3 证明中的方法，可知 $q$ 的素因子 $p$ 不等于 $p_1,p_2,\cdots,p_k$ 中的任何一个. 而 $p_1,p_2,\cdots,p_k$ 是所有不超过 $n$ 的素数，因此 $p>n$ ，所以 $n<p\leqslant q<n\,!$.

从而，命题成立.

说明利用本题的结论亦可证出：素数有无穷多个. 贝特朗曾猜测在 $m>1$ 时，正整数 $m$ 与 $2m$ 之间（不包括 $m$ 与 $2m$ ）有一个素数. 如果将素数从小到大排列为 $p_1<p_2<\cdots$ ，该猜测亦即 $p_{n+1}<2p_n$ . 这个猜测被契比雪夫证明了. 因此它被称为贝特朗猜想或契比雪夫定理.

例 6 设 $a,b,c,d,e,f$ 都是正整数，$S=a+b+c+d+e+f$ 是 $abc+def$ 和 $ab+bc+ca-de-ef-ed$ 的因数. 证明: $S$ 为合数.

证明考虑多项式

$$f(x)=(x+a)(x+b)(x+c)-(x-d)(x-e)(x-f)$$

展开后, 可知

$$f(x)=Sx^2+(ab+bc+ca-de-ef-fd)x+(abc+def)$$

由条件可知，对任意 $x\in\mathbf{Z}$ ，都有 $S\mid f(x)$ . 特别地，取 $x=d$ ，就有 $S\mid f(d)$ ，即 $S\mid(d+a)(d+b)(d+c)$ . 由于 $a,b,c,d,e,f$ 都为正整数，故 $d+a,d+b$ , $d+c$ 都小于 $S$, 所以, $S$ 为合数.

说明对比例 2，两个例子中分别用到下面的结论：若 $x,y,z$ 为正整数，且 $\frac{xy}{z}$ 亦为整数, 则如果 $x,y>z$, 那么 $\frac{xy}{z}$ 为合数; 如果 $x,y<z$, 那么 $z$ 为合数.

### 1.1.3 最大公因数与最小公倍数

设 $a,b$ 是不全为零的两个整数, $d$ 是一个非零整数，如果 $d\mid a$ 且 $d\mid b$ ，那么称 $d$ 为 $a,b$ 的公因数.

注意到，当 $d\mid a$ 且 $d\mid b$ 时，则 $d\leqslant|a|$ 或 $d\leqslant|b|$ 中必有一个成立（对 $a,b$ 中不为零的数成立). 因此, $a,b$ 的公因数中有一个最大的, 这个数称为 $a,b$ 的最大公因数，记为 $(a,b)$ . 如果 $(a,b)=1$ ，那么我们称 $a,b$ 互素.

在讨论最大公因数的性质之前，我们不加证明地引入一个在小学就接触到的, 数论中最基本, 最常用的结论.

带余数除法设 $a, b$ 是两个整数, $a \neq 0$, 则存在唯一的一对整数 $q$ 和 $r$, 满足

$$b = aq + r, 0 \leqslant r < |b|$$

其中 $q$ 称为 $b$ 除以 $a$ 所得的商, $r$ 称为 $b$ 除以 $a$ 所得的余数.
性质 1 设 $d = (a, b)$ ，则存在整数 $x, y$ ，使得

$$ax + by = d$$

这个结论就是著名的贝祖（Bezout）定理.
证明我们利用带余除法来处理，此结论的证明过程又是求 $a, b$ 的最大公因数的过程，它被称为" 辗转相除".

不妨设 $a, b$ 都不为零（当 $a, b$ 中有一个为零时，结论是显然的)，且 $|a| \leqslant |b|$.

设 $b = aq_1 + r_1$, 其中 $0 \leqslant r_1 < |a|, q_1, r_1$ 为整数. 若 $r_1 = 0$ ，则辗转相

除到此为止; 否则用 $a$ 去除以 $r_1$, 得等式 $a = r_1 q_2 + r_2, 0 \leqslant r_2 < r_1$; 依此讨论, 由于 $r_1 > r_2 > r_3 > \cdots$, 因此辗转相除到某一步后, 所得的 $r_{k+1} = 0$, 于是, 我们得到了如下的一系列式子:

$$b = aq_1 + r_1, 0 < r_1 < |a| \tag{1.17}$$

$$a = r_1 q_2 + r_2, 0 < r_2 < r_1 \tag{1.18}$$

$$r_1 = r_2 q_3 + r_3, 0 < r_3 < r_2 \tag{1.19}$$

$$\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \tag{1.20}$$

$$r_{k-2} = r_{k-1} q_k + r_k, 0 < r_k < r_{k-1} \tag{1.21}$$

$$r_{k-1} = r_k q_{k+1} \tag{1.22}$$

注意到, 从第一个式子到第 $k$ 个式子, 我们依次有

$$d \,|r_1, d|\, r_2, \cdots, d \mid r_k,$$

而从第 $k+1$ 个式子倒推, 又依次有

$$r_k \,|r_{k-1}, r_k|\, r_{k-2}, \cdots, r_k \,|r_1, r_k|\, a, r_k \mid b,$$

所以, $r_k$ 又是 $a,b$ 的公因数, 结合 $d$ 为 $a,b$ 的最大公因数知 $r_k \leqslant d$, 又 $d \mid r_k$, 故 $d \leqslant r_k$, 因此, $d = r_k$ . 也就是说, 我们求出了 $a,b$ 的最大公因数.

现在, 利用 $d = r_k$ 及第 $k$ 个式子, 可知

$$d = r_{k-2} - r_{k-1}q_k$$

再由

$$r_{k-1} = r_{k-3} - r_{k-2}q_{k-1}(\text{ 第}k-1\text{ 个式子变形得}),$$

代入上式, 可知 $d$ 可以表示为 $r_{k-2}$ 与 $r_{k-3}$ 的" 线性组合" (见 1.1 节性质 2), 依此倒推, 可知 $d$ 可以表示为 $a,b$ 的" 线性组合", 即存在整数 $x,y$ 使得

$$d = ax + by.$$

说明反过来, 设 $x,y$ 为整数, $d' = ax + by$, 并不能推出 $d'$ 为 $a,b$ 的最大公因数. 事实上, 可以证明: $a,b$ 的最大公因数是形如 $ax + by$（$x,y$ 为任意整数) 的正整数中最小的那个.

性质 2 设 $d$ 为 $a,b$ 的公因数, 则 $d \mid (a,b)$ .
这个性质可由前面的贝祖定理证出. 事实上, 贝祖定理也是初等数论中的一个基本定理，应用非常广泛，下面的性质是它的一个直接推论.

性质 3 设 $a,b$ 是不全为零的整数, 则 $a$ 与 $b$ 互素的充要条件是存在整数 $x,y$ 满足

$$ax + by = 1$$

性质 4 设 $a|c, b|c$ ，且 $(a,b) = 1$ ，则 $ab \mid c$ .
这个性质的证明见 1.1 节的例 1.
性质 5 设 $a \mid bc$ ，且 $(a,b) = 1$ ，则 $a \mid c$ .
证明由性质 3，知存在整数 $x,y$ 使得

$$ax + by = 1$$

故 $acx+bcy=c$ ，由 $a\mid bc$ 及 $a\mid acx$ ，可知 $a\mid c$ .

性质 6 设 $p$ 为素数，$p\mid ab$ ，则 $p\mid a$ 或 $p\mid b$ .

证明由于 $p$ 只有两个正约数，故 $(p,a)=1$ 或者 $(p,a)=p$ . 若 $(p,a)=1$ ，则由性质 5 知 $p\mid b$ ；若 $(p,a)=p$ ，则 $p\mid a$ .

下面引入公倍数的一些概念和性质.

设 $a,b$ 都是不等于零的整数，如果整数 $c$ 满足 $a\mid c$ 且 $b\mid c$ ，那么称 $c$ 为 $a,b$ 的公倍数. 在 $a,b$ 的所有正的公倍数中，最小的那个称为 $a,b$ 的最小公倍数，记作 $[a,b]$ .

性质 7 设 $a,b$ 为非零整数, $d,c$ 分别是 $a,b$ 的一个公因数与公倍数, 则 $d|(a,b),[a,b]|c$ .

证明这个性质在本质上反映了最大公因数与最小公倍数的属性. 前者是性质 2 的结论，这里再次列出是为了对比.

对于后者，采用反证法予以证明.

若 $[a,b]\nmid c$ ，设 $c=[a,b]\cdot q+r,0<r<[a,b]$ ，则由 $a\mid c$ 及 $a\mid[a,b]$ ，可知 $a\mid r$ ，同理 $b\mid r$ ，即 $r$ 为 $a,b$ 的公倍数，但 $r<[a,b]$ ，这与 $[a,b]$ 是 $a,b$ 的最小公倍数矛盾. 所以 $[a,b]\mid c$ .

性质 8 设 $a,b$ 都是正整数, 则 $[a,b]=\frac{ab}{(a,b)}$.

证明记 $c=\frac{ab}{(a,b)}$, 则由 $(a,b)\mid a$ 及 $(a,b)\mid b$ 知 $b|c,a|c$ . 即 $c$ 为 $a,b$ 的公倍数，故 $[a,b]\mid c$ .

反过来，由贝祖定理，知存在整数 $x,y$ ，使得

即

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

$$\frac{a}{(a,b)}x+\frac{b}{(a,b)}y=1$$

于是

$$\frac{a[a,b]}{(a,b)}x+\frac{b[a,b]}{(a,b)}y=[a,b]$$

由 $b\mid[a,b]$ 及 $a\mid[a,b]$, 可知

$$c\left|\frac{a[a,b]}{(a,b)},c\right|\frac{b[a,b]}{(a,b)}$$

所以

$$c \mid [a, b]$$

综上, 可知

$$[a, b] = \frac{ab}{(a, b)}$$

一般地，对 $n$ 个整数（非零）$a_1, a_2, \cdots, a_n$，可以类似地引入最大公因数与最小公倍数的概念，分别记为 $(a_1, a_2, \cdots, a_n)$ 和 $[a_1, a_2, \cdots, a_n]$. 容易得到下面的一些结论：

性质 9 $(a_1, a_2, a_3, \cdots, a_n) = \left((a_1, a_2), a_3, \cdots, a_n\right)$；而 $[a_1, a_2, a_3, \cdots, a_n] = \left[[a_1, a_2], a_3, \cdots, a_n\right]$.

性质 10 存在整数 $x_1, x_2, \cdots, x_n$， 使得

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = (a_1, a_2, \cdots, a_n)$$

特别地，$(a_1, a_2, \cdots, a_n) = 1$，即 $a_1, a_2, \cdots, a_n$ 互素的充要条件是：存在整数 $x_1, x_2, \cdots, x_n$, 使得

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = 1$$

注意，$n$ 个数互素，并不能保证它们两两互素，例如（$2\times 3, 2\times 5, 3\times 5$ $= 1$，但 6, 10, 15 两两不互素. 反过来，若 $n$ 个数中有两个数互素，则这 $n$ 个数互素. 因此，在 $n$ 个数中，" 两两互素" 的条件比" 它们互素" 的条件要强得多.

性质 11 设 $m$ 为正整数, 则

$$(ma_1, ma_2, \cdots, ma_n) = m\,(a_1, a_2, \cdots, a_n) \tag{1.23}$$

$$[ma_1, ma_2, \cdots, ma_n] = m\,[a_1, a_2, \cdots, a_n] \tag{1.24}$$

例 1 设 $a, b$ 为正整数，且 $\frac{ab}{a+b}$ 也是正整数. 证明：$(a, b) > 1$ .

证明若 $(a, b) = 1$，则 $(a, a+b) = 1$（这由性质 3 可推得），从而，由 $a+b \mid ab$ 及 $(a, a+b) = 1$，得 $a+b \mid b$，但是 $a+b > b$，故 $a+b \mid b$ 不可能成立. 所以，$(a, b) > 1$.

说明在辗转相除求 $a, b$ 的公因数的讨论中，可知对任意整数 $x$ ，都有 $(a, b)=(a, b+a x)$, 这一点在利用最大公因数处理数论问题时经常被用到.

例 2 设正整数 $a, b, c$ 满足 $b^{2}=a c$ . 证明: $(a, b)^{2}=a(a, c)$.

证明如果我们能够证明：$(a, b)^{2}=\left(a^{2}, b^{2}\right)$ ，那么结合性质 11，可知

$$(a, b)^{2}=\left(a^{2}, b^{2}\right)=\left(a^{2}, a c\right)=a(a, c)$$

命题获证.

为此，记 $d=(a, b)$ ，设 $a=d u, b=d v$ ，则由性质 11 可知 $u, v$ 是两个互素的正整数，为证 $\left(a^{2}, b^{2}\right)=d^{2}$ ，只需证明：$\left(u^{2}, v^{2}\right)=1$ .

利用贝祖定理，知存在整数 $x, y$ ，使得 $u x+v y=1$ ，故 $u^{2} x^{2}=(1-v y)^{2}=1+v\left(v y^{2}-2 y\right)$ ，结合性质 3 可知 $\left(u^{2}, v\right)=1$ ，交换 $u^{2}$ 与 $v$ 的位置，同上再做一次，即有 $\left(v^{2}, u^{2}\right)=1$ .

所以，命题成立.

说明利用下一节的算术基本定理可以非常方便地证出：$\left(a^{2}, b^{2}\right)=(a, b)^{2}$ ，但遗憾的是我们还没给出该定理的证明，通常都是先建立最大公因数理论再去证算术基本定理，这里不用该定理是不希望掉入” 循环论证” 的旋涡，读者在学习中应认真掌握其中的逻辑结构.

例 3 求所有的正整数 $a, b(a \leqslant b)$ ，使得

$$a b=300+7[a, b]+5(a, b)$$

解设 $[a, b]=x,(a, b)=y$ ，由性质 8 可知 $a b=x y$ ，于是，(1) 变为

$$x y=300+7 x+5 y$$

即 $(x-5)(y-7)=5 \times 67$ .

由于 $[a, b] \geqslant(a, b)$, 故 $x \geqslant y$, 进而 $x-5>y-7$, 只有如下的两种情形.

情形一 $x-5=67$ 且 $y-7=5$ ；此时，$x=72, y=12$ ，于是，可设 $a=12 n$ $b=12 m$ $(m, n)=1$ ，并有 $(12 n)(12 m)=a b=x y=12 \times 72$ ，结合 $a \leqslant b$ ，只能是 $(m, n)=(1,6)$ 或 $(2,3)$ ，对应的 $(a, b)=(12,72)$ 或 (24 ，36).

情形二　$x-5=335$ 且 $y-7=1$ ；对应地，$x=340, y=8$ ，但 $y=(a$　$b$　是 $x=[a, b]$ 的因数, 而 $8 \nmid 340$ ，所以，此时无解.

综上，符合条件的 $(a,b)=(12,72)$ 或 $(24,36)$ .
例 4 求所有的正整数 $a,b$, 使得

$$(a,b)+9[a,b]+9(a+b)=7ab$$

解记 $(a,b)=d$ ，设 $a=dx,b=dy$ ，则 $(x,y)=1$ （由性质 11 知），$[a,b]=dxy$ （由性质 8 知），于是代入 (1) 可得

$$1+9xy+9(x+y)=7dxy$$

$$7d=9+9\left(\frac{1}{x}+\frac{1}{y}\right)+\frac{1}{xy}$$

所以

$$9<7d\leqslant 9+9\left(\frac{1}{1}+\frac{1}{1}\right)+\frac{1}{1\times 1}=28$$

故

$$2\leqslant d\leqslant 4$$

当 $d=2$ 时, 由 (2) 得

$$5xy-9(x+y)=1$$

两边乘以 5 ，并将左边因式分解，得

$$(5x-9)(5y-9)=86=2\times 43$$

故 $(5x-9,5y-9)=(1,86),(86,1),(2,43),(43,2)$. 分别求解可知只能是 $(x,y)=(2,19),(19,2)$ ，对应的 $(a,b)=(4,38),(38,4)$ .

分别就 $d=3,4$ 同上讨论，得 $(a,b)=(4,4)$ .
所以，满足条件的 $(a,b)=(4,38),(38,4),(4,4)$ .

例 5 Fibonacci 数列定义如下：$F_1=F_2=1, F_{n+2}=F_{n+1}+F_n, n=1$ ，$2,\cdots$ . 证明：对任意正整数 $m,n$ ，都有 $(F_m,F_n)=F_{(m,n)}$ .

证明当 $m=n$ 时，命题显然成立. 现在不妨设 $m<n$ ，注意到

$$\begin{aligned}
F_n &= F_2F_{n-1}+F_1F_{n-2} && (1.25)\\
&= F_2\left(F_{n-2}+F_{n-3}\right)+F_1F_{n-2} && (1.26)\\
&= \left(F_2+F_1\right)F_{n-2}+F_2F_{n-3} && (1.27)\\
&= F_3F_{n-2}+F_2F_{n-3} && (1.28)\\
&= F_3\left(F_{n-3}+F_{n-4}\right)+F_2F_{n-3} && (1.29)\\
&= F_4F_{n-3}+F_3F_{n-4} && (1.30)\\
&= \cdots && (1.31)\\
&= F_mF_{n-m+1}+F_{m-1}F_{n-m}, && (1.32)
\end{aligned}$$

因此, 设 $d\mid F_m$ 且 $d\mid F_n$, 则由上式可知 $d\mid F_{m-1}F_{n\to m}$. 又对任意正整数 $m$ ，有 $(F_m,F_{m-1})=(F_{m-1}+F_{m-2},F_{m-1})=(F_{m-1},F_{m-2})=\cdots=(F_2,F_1)=1$, 所以, $(d,F_{m-1})=1$, 故 $d\mid F_{n-m}$; 反过来, 若 $d'\mid F_{n-m}$ 且 $d'\mid F_m$, 则由上式又可知 $d'\mid F_n$ . 依此可知 $(F_n,F_m)=(F_{n-m},F_m)$ .

利用上述结论, 对下标进行辗转相除, 就可证得 $(F_n,F_m)=F_{(m,n)}$.
说明由本题的结论还可以推出一个有趣的性质: 若 $F_n$ 为素数, 则 $n=4$ 或者 $n$ 为素数.

事实上, 设 $F_n$ 为素数, 而 $n$ 为合数, 可设 $n=p\cdot q, 2\leqslant p\leqslant q, p,q$ 为正

整数, 则由前面的结论, 可知 $\left(F_n,F_p\right)=F_{(n,p)}=F_p, \left(F_n,F_q\right)=F_{(n,q)}=F_q$ . 结合 Fibonacci 数列的定义，可知 $F_n>F_p, F_n>F_q$ ，而 $F_n$ 为素数，故 $\left(F_n,F_p\right)=\left(F_n,F_q\right)=1$ ，所以，$F_p=F_q=1$ ，再由 $2\leqslant p\leqslant q$ ，可知只能是 $p=q=2$ ，即 $n=4$ . 所以，性质成立.

例 6 设 $n$ 为大于 1 的正整数. 证明：存在从小到大排列后成等差数列 (即从第二项起, 每一项与它前面那项的差为常数的数列) 的 $n$ 个正整数，它们中任意两项互素.

证明考虑下面的 $n$ 个数：

$$n!+1, 2\times(n!)+1, \cdots, n\times(n!)+1$$

这 $n$ 个正整数组成一个公差为 $n!$ 的等差数列.
我们证明其中任意两项是互素的.

事实上，若存在 $1 \leqslant i < j \leqslant n$ ，使得数 $i \times (n!) + 1$ 与数 $j \times (n!) + 1$ 不互素，设 $d = (i \times (n!) + 1, j \times (n!) + 1) > 1$ . 考虑 $d$ 的素因子 $p$ ，可知

$$p \mid (j \times (n!) + 1) - (i \times (n!) + 1)$$

即 $p \mid (j-i) \times n\,!$. 由性质 6 知 $p \mid j-i$ 或 $p \mid n!$，结合 $1 \leqslant j-i < n$ ，可知 $(j-i) \mid n!$ ，所以，总有 $p \mid n!$ . 但是，$p|d, d|i \times (n!) + 1$ ，故 $p \mid i \times (n!) + 1$ ，结合 $p \mid n!$ ，导致 $p \mid 1$ ，矛盾.

所以，命题成立.

说明此题为导出与反设矛盾的结论，采用了素因子分析的方法. 该方法在数论中有广泛的应用.

### 1.1.4　算术基本定理

在 1.2 节中我们引入了素数与合数的概念，对每个大于 1 的正整数 $n$ ，如果 $n$ 为合数，那么可写 $n = n_1 n_2$ ，其中 $2 \leqslant n_1 \leqslant n_2$ . 再分别对 $n_1, n_2$ 重复这样的讨论，即可将 $n$ 表示为一些素数的乘积. 对这个过程认真思考，就能得到下面的重要定理，在解数论的问题时经常会直接或间接地用到它.

算术基本定理设 $n$ 是大于 1 的正整数，则 $n$ 可以分解成若干个素数的乘积的形式，并且在不考虑这些素数相乘时的前后次序时，这种分解是唯一的. 即对任意大于 1 的正整数 $n$, 都存在唯一的一种素因数分解形式:

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

这里 $p_1 < p_2 < \cdots < p_k$ 为素数，$\alpha_1, \alpha_2, \cdots, \alpha_k$ 为正整数.

证明利用前面的分析，可证得存在性，下面证明唯一性.

若 $n$ 有两种素因数分解形式:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_2}$$

其中 $p_1 < p_2 < \cdots < p_k, q_1 < q_2 < \cdots < q_l$ ，且都是素数，$\alpha_i, \beta_j$ 都为正整数，$1 \leqslant i \leqslant k, 1 \leqslant j \leqslant l$.

我们证明 $k = l$ 且 $p_i = q_i, \alpha_i = \beta_i$ .

事实上，由 (1) 知 $p_i \mid q_1^{\beta_1} q_2^{\beta_2} \cdots q_l^{\beta_l}$ ，利用前一节的性质 6 可知，存在

某个 $j$ 使 $p_i \mid q_j^{\beta_j}$ ，再用一次性质 6，知 $p_i \mid q_j$ ，这要求 $p_i = q_j$ . 即对 $1 \leqslant i \leqslant k$ 及每个 $p_i$ ，在 $q_1, q_2, \cdots, q_l$ 中总有一个 $q_j$ ，使得 $p_i = q_j$ . 反过来对 $q_j$ 分析，又有对 $1 \leqslant j \leqslant l$ 及每个 $q_j$ ，在 $p_1, p_2, \cdots, p_k$ 中总有一个 $p_i$ ，使得 $q_j = p_i$ . 这表明 $k = l$ ，且 $q_1, q_2, \cdots, q_l$ 是 $p_1, p_2, \cdots, p_k$ 的一个排列，结合 $p_1 < p_2 < \cdots < p_k$ 及 $q_1 < q_2 < \cdots < q_l$ ，知 $p_i = q_i, 1 \leqslant i \leqslant k$ . 进一步证明 $\alpha_i = \beta_i$ 是容易的.

利用正整数 $n$ 的素因数分解式，我们可以简单地得到下面的一些结论.

$1^\circ$ 设 $n$ 的所有正因数（包括 1 和 $n$ ）的个数为 $d(n)$ ，那么

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

由此公式易知: $n$ 是一个完全平方数的充要条件是 $d(n)$ 为奇数.

$2^\circ$ 设 $n$ 的所有正因数之和为 $\sigma(n)$ ，那么

$$\sigma(n) = (1 + p_1 + \cdots + p_1^{\alpha_1})(1 + p_2 + \cdots + p_2^{\alpha_2}) \cdots \left(1 + p_k + \cdots + p_k^{\alpha_k}\right)$$

由此可知：$\sigma(n)$ 为奇数的充要条件是 $n$ 为完全平方数或者某个完全平方数的两倍.

$3^\circ$ 设 $n, m$ 的素因数分解分别为

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

这里 $p_1 < p_2 < \cdots < p_k$ ，都为素数，$\alpha_i, \beta_i$ 都是非负整数，并且对每个 $1 \leqslant i \leqslant k, \alpha_i$ 与 $\beta_i$ 不全为零，那么，我们有 $(m, n) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$ ；$[m, n] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}$ ，其中 $\gamma_i = \min\{\alpha_i, \beta_i\}, \delta_i = \max\{\alpha_i, \beta_i\}, 1 \leqslant i \leqslant k$ .

例 1 在一个走廊上依次排列着编号为 $1, 2, \cdots, 2012$ 的灯共 2012 盏，最初每盏灯的状态都是开着的. 一个好动的学生做了下面的 2012 次操作：对 $1 \leqslant k \leqslant 2012$ ，该学生第 $k$ 次操作时，将所有编号是 $k$ 的倍数的灯的开关都拉了一下. 问: 最后还有多少盏灯是开着的?

解设 $1 \leqslant n \leqslant 2012$ ，我们来考察第 $n$ 盏灯的状态，依题意，该盏灯的开关被拉了 $d(n)$ 次. 而偶数次拉动开关不改变灯的初始状态，奇数次拉动开关，

灯的状态与初始状态不同.

利用 $d(n)$ 的性质及前面的讨论, 因为 $1, 2, \cdots, 2012$ 中恰有 44 个数为完全平方数, 可知最后还有 $2012 - 44 = 1968$ 盛灯是开着的.

例 2 求所有的正整数 $n$, 使得 $n=d(n)^2$ .
解当 $n=1$ 时, 符合条件, 下面考虑 $n>1$ 的情形.
由条件知 $n$ 为完全平方数, 因此 $d(n)$ 为奇数, 设 $d(n)=2k+1$. 鉴于对任意正整数 $d$, 当 $d\mid n$ 时, 有 $\left.\frac{n}{d}\right| n$, 因此, 我们将 $d$ 与 $\frac{n}{d}$ 配对后, 可知 $d(n)$ 等于数 $1,2,\cdots,2k-1$ 中为 $n$ 的因数的个数的两倍加上 1 . 又 $1,2,\cdots,2k-1$ 中的偶数都不是 $n\left(=(2k+1)^2\right)$ 的因数, 因此结合 $d(n)=2k+1$, 可知 1 , $2,\cdots,2k-1$ 中的每一个奇数都是 $n$ 的因数.

注意到, 当 $k>1$ 时, $(2k-1,2k+1)=(2k-1,2)=1$, 故 $2k-1\nmid(2k+1)^2$. 所以 $k>1$ 时, $n=(2k+1)^2$ 不符合要求, 故 $k=1,n$ 只能等于 9 .

直接验证, 可知 1 和 9 满足条件, 所以 $n=1$ 或 9.
说明此题考虑了 $n$ 的因数关于 $\sqrt{n}$ 的对称性, 分析出一个非常强的条件, 从而解决了问题.

它还有一个一般性的处理方法, 需要用到如下的估计: 设 $p$ 为不小于 5 的素数, 则 $p^\alpha>(\alpha+1)^2$. 而 $\alpha\geqslant 2$ 时, $3^\alpha\geqslant(\alpha+1)^2$. 这两个不等式都可以用数学归纳法予以证明（对 $\alpha$ 归纳）.

现在设 $n(>1)$ 是一个满足条件的正整数, 则 $n$ 为一个奇数的平方, 于是, 可设 $n=3^\alpha\cdot p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$, 其中 $3<p_1<p_2<\cdots<p_k$, 并且 $\alpha,\beta_1$, $\beta_2,\cdots,\beta_k$ 都是偶数. 如果 $k>0$, 那么由前面的分析, 知 $n>(\alpha+1)^2\left(\beta_1+1\right)^2\cdot\left(\beta_2+1\right)^2\cdots\left(\beta_k+1\right)^2=d(n)^2$, 矛盾, 故 $n=3^\alpha$. 进一步分析, 可知 $\alpha>2$ 时, 有 $3^\alpha>(\alpha+1)^2$ 故 $\alpha=2$, 即 $n=9$.

例 3 设 $n$ 为正整数. 证明: 数 $2^{2^n}+2^{2^{n-1}}+1$ 至少有 $n$ 个不同的素因子. 证明我们作如下的分解:

$$
\begin{aligned}
& 2^{2^n}+2^{2^{n-1}}+1 && (1.33)\\
= & \left(2^{2^{n-1}}+1\right)^2-2^{2^{n-1}} && (1.34)\\
= & \left(2^{2^{n-1}}+2^{2^{n-2}}+1\right)\left(2^{2^{n-1}}-2^{2^{n-2}}+1\right) && (1.35)\\
= & \left(2^{2^{n-2}}+2^{2^{n-3}}+1\right)\left(2^{2^{n-2}}-2^{2^{n-3}}+1\right)\left(2^{2^{n-1}}-2^{2^{n-2}}+1\right) && (1.36)\\
= & \cdots && (1.37)\\
= & \left(2^{2^1}+2^{2^0}+1\right)\left(2^{2^1}-2^{2^0}+1\right)\left(2^{2^2}-2^{2^1}+1\right)\cdots\left(2^{2^{n-1}}-2^{2^{n-2}}+1\right) && (1.38)
\end{aligned}
$$

这样, 我们将 $2^{2^n}+2^{2^{n-1}}+1$ 表示为 $n$ 个大于 1 的正整数之积, 为证明它有 $n$ 个不同的素因子，只需证明这 $n$ 个大于 1 的正整数两两互

素.

注意到, 当 $m > l$ 时, $2^{2^l}+2^{2^{L-1}}+1$ 与 $2^{2^l}-2^{2^{L-1}}+1$ 都是 $2^{2^m}+2^{2^{m-1}}+1$ 的因数, 因此

$$\left(2^{2^m}-2^{2^{m-1}}+1, 2^{2^l}\pm 2^{2^{L-1}}+1\right) \tag{1.39}$$
$$\leqslant\left(2^{2^m}-2^{2^{m-1}}+1, 2^{2^m}+2^{2^{m-1}}+1\right) \tag{1.40}$$
$$=\left(2^{2^m}-2^{2^{m-1}}+1, 2\times 2^{2m-1}\right) \tag{1.41}$$

由于, $2\times 2^{2m-1}$ 中只有一个素因子 2 , 而 $2^{2^m}-2^{2^{m-1}}+1$ 为奇数, 故

因此

$$\left(2^{2^m}-2^{2^{m-1}}+1, 2\times 2^{2^{m-1}}\right)=1,$$

$$\left(2^{2^m}-2^{2m-1}+1, 2^{2^l}\pm 2^{2^{2-1}}+1\right)=1.$$

所以, $2^{2^1}+2^{2^0}+1, 2^{2^1}-2^{2^0}+1, 2^{2^2}-2^{2^1}+1,\cdots, 2^{2^{n-1}}-2^{2^{n-2}}+1$ 两两互素, 进而 $2^{2^n}+2^{2^{n-1}}+1$ 至少有 $n$ 个不同的素因子.

例 4 设 $m,n$ 是正整数, 且 $m$ 的所有正因数之积等于 $n$ 的所有正因数之积. 问: $m$ 与 $n$ 是否必须相等?

解 $m$ 与 $n$ 必须相等.

事实上, 将 $m$ 的正因数 $d$ 与 $\frac{m}{d}$ 配对, 可知 $m$ 的所有正因数之积为 $m\frac{d(m)}{2}$, 因此, 条件等价于

$$m^{d(n)}=n^{d(n)},$$

此式表明 $m,n$ 有相同的素因子, 可设

$$m=p_1^{a_1}p_2^{a_2}\cdots p_k^{\alpha_k}, n=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k},$$

其中 $p_1<p_2<\cdots<p_k$ 为素数 $\alpha_i$ 与 $\beta_i$ 都是正整数, $1\leqslant i\leqslant k$.
代入 (1) 式, 利用算术基本定理, 可知

$$\alpha_i d(m)=\beta_i d(n), 1\leqslant i\leqslant k,$$

若 $d(m)>d(n)$, 则对 $1 \leqslant i \leqslant k$, 都有 $\alpha_i<\beta_i$, 于是, $\alpha_i+1<\beta_i+1$, 故 $\left(\alpha_1+1\right)\left(\alpha_2+1\right) \cdots\left(\alpha_k+1\right)<\left(\beta_1+1\right)\left(\beta_2+1\right) \cdots\left(\beta_k+1\right)$, 这导致 $d(m)<d(n)$ ，矛盾. 同样，由 $d(m)<d(n)$ ，利用 (2) 式也可导出矛盾. 所以 $d(m)=d(n)$ ，进而由 (1) 式得 $m=n$.

说明一般地, 由 $\sigma(m)=\sigma(n)$ (即考虑 $m, n$ 所有正因数之和) 并不能导出 $m=n$ (例如 $\sigma(6)=\sigma(11)=12$ ), 此题是对两个正整数的所有正因数作乘积方面的思考得出的结论.

例 5 求所有的正整数 $x, y$, 使得

$$
y^x=x^{50}
$$

解设 $x, y$ 为满足条件的正整数，并且 $x=p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ 为 $x$ 的素因数分解式，则

由 $y$ 为正整数，知对 $1 \leqslant i \leqslant k$ ，都有 $x \mid 50 \alpha_i$ . 现在先讨论 $x$ 的素因子.

如果 $x$ 有一个不同于 2 和 5 的素因子 $p$ ，并设 $p^\alpha \| x$ ，那么由前面的结果知 $x \mid 50 \alpha$ ，当然有 $p^\alpha \mid 50 \alpha$ ，又 $p \neq 2,5$ ，故 $p^\alpha \mid \alpha$ . 但是，对任意素数 $p$ 及正整数 $\alpha$ ，有 $p^\alpha>\alpha$ ，所以，$p^\alpha \mid \alpha$ 不能成立，这表明 $x$ 的素因子只能为 2 或 5 .

于是，我们可设 $x=2^\alpha \cdot 5^\beta$ （其中 $\alpha, \beta$ 为非负整数），这时 $x|50 \alpha, x| 50 \beta$ ，故 $2^\alpha\left|50 \alpha, 5^\beta\right| 50 \beta$ ，前者要求 $2^{\alpha-1} \mid \alpha$ ，后者要求 $5^{\beta-2} \mid \beta$ . 注意到，当 $\alpha \geqslant 3$ 时，$2^{\alpha-1}>\alpha$, 而 $\beta \geqslant 3$ 时, $5^{\beta-2}>\beta$ ，所以，$0 \leqslant \alpha \leqslant 2,0 \leqslant \beta \leqslant 2$ . 这表明 $x$ 只能取 $1,2,2^2, 5,5^2, 2 \times 5,2^2 \times 5,2 \times 5^2, 2^2 \times 5^2$ .

将 $x$ 的上述取值逐个代入 (1) 式，可得到全部解为 $(x, y)=(1,1)$ ，$\left(2,2^{25}\right),\left(2^2, 2^{25}\right),\left(5,5^{10}\right),\left(5^2, 5^4\right),\left(10,10^5\right),(50,50),(100,10)$, 共 8 组解.

说明上面两例直接用到算术基本定理，所涉及的变量数看似增加或会变难，但这时不等式估计的手段可介入，问题求解反而有了着力点.

例 6 给定正整数 $n>1$ ，设 $d_1, d_2, \cdots, d_n$ 都是正整数，满足：$\left(d_1, d_2, \cdots，d_n\right)=1$ ，且对 $j=1,2, \cdots, n$ 都有 $d_j \mid \sum_{i=1}^n d_i$( 这里 $\sum_{i=1}^n d_i=d_1+d_2+\cdots+ d_n$).

（1）证明: $d_1 d_2 \cdots d_n \mid\left(\sum_{i=1}^n d_i\right)^{n-2}$ ；

（2）举例说明：$n>2$ 时，上式右边的幂次不能减小.

证明（1）设 $p$ 为 $d_1 d_2 \cdots d_n$ 的素因数，且 $k$ 为各 $d_i$ 的素因数分解式中 $p$ 的幂次的最大值, 则由 $d_j \mid \sum_{i=1}^n d_i$ 可知, $p^k \mid \sum_{i=1}^n d_i$, 故 $p^{k(n-2)} \mid \left(\sum_{i=1}^n d_i\right)^{n-2}$.

而 $(d_1,d_2,\cdots,d_n)=1$，故存在 $d_i$，使得 $p\nmid d_i$，结合 $p\mid\sum_{i=1}^{n}d_i$，可知 $d_1$，$d_2,\cdots,d_n$ 中至少有两个数不是 $p$ 的倍数. 所以, $p$ 在 $d_1d_2\cdots d_n$ 中的幂次不超过 $k(n-2)$，依此可知结论成立.

（2）设 $d_1=1,d_2=n-1,d_i=n,3\leqslant i\leqslant n$，则 $\sum_{i=1}^{n}d_i=n(n-1)$ 是每个 $d_i$ 的倍数，且 $(d_i,d_2,\cdots,d_n)=1$.

此时，$d_1d_2\cdots d_n=n^{n-2}(n-1)$，结合 $(n,n-1)=1$，可知满足 $n^{n-2}(n-1)\mid(n(n-1))^m$ 的最小正整数 $m=n-2$.

### 1.1.5　习题 1

1 设 $n$ 为大于 1 的正整数. 证明：$n^4+4^n$ 是一个合数.

2 求使得 $\left|4x^2-12x-27\right|$ 为素数的所有整数 $x$ .

3 设 $m$ 为大于 1 的正整数，且 $m\mid(m-1)!+1$ . 证明：$m$ 是一个素数.

4 是否存在 3 个不同的素数 $p,q,r$，使得下面的整除关系都成立？

$$qr\left|p^2+d,rp\right|q^2+d,pq\mid r^2+d$$

其中（1）$d=10$  2 $d=11$ .

5 设 $p$ 为正整数，且 $2^p-1$ 是素数. 求证：$p$ 为素数.

6 设 $n$ 为正整数，且 $2^n+1$ 是素数. 证明：存在非负整数 $k$，使得 $n=2^k$ .

7 求所有形如 $n^n+1$ 且不超过 $10^{19}$ 的素数，这里 $n$ 为正整数.

8 设 $a,b,c,d$ 都是整数，且 $a\neq c,a-c\mid ab+cd$ . 证明：$a-c\mid ad+bc$ .

9 设 $a,b,c,d$ 为整数，且 $ac,bc+ad,bd$ 都是某个整数 $u$ 的倍数. 证明：数 $bc$ 和 $ad$ 也是 $u$ 的倍数.

10 设 $a,b,n$ 为给定的正整数，且对任意正整数 $k(\neq b)$，都有 $b-k\mid a-k^n$ . 证明: $a=b^n$ .

11 已知正整数 $n$ 的正因数中，末尾数字为 $0,1,2,\cdots,9$ 的正整数都至少有一个. 求满足条件的最小的 $n$ .

12 求一个 9 位数 $M$，使得 $M$ 的数码两两不同且都不为零，并对 $m=2,3,\cdots$，9，数 $M$ 的左边 $m$ 位数都是 $m$ 的倍数.

13 对于一个正整数 $n$，若存在正整数 $a,b$，使得 $n=ab+a+b$，则称 $n$ 是一个" 好数"，例如 $3=1\times1+1+1$，故 3 为一个" 好数". 问：在 $1,2,\cdots,100$ 中，有多少个" 好数"？

14 设素数从小到大依次为 $p_1,p_2,p_3,\cdots$ . 证明：当 $n\geqslant2$ 时，数 $p_n+p_{n+1}$ 可以表示为 3 个大于 1 的正整数（可以相同）的乘积的形式.

15 设 $n$ 为大于 1 的正整数. 证明：$n$ 为合数的充要条件是存在正整数 $a, b$ , $x, y$ ，使得 $n = a + b, \frac{x}{a} + \frac{y}{b} = 1$ .
16 证明：数列 $10001, 100010001, 1000100010001, \cdots$ 中，每一个数都是合数.

17 设 $a, b, c, d$ 都是素数，且 $a > 3b > 6c > 12d, a^2 - b^2 + c^2 - d^2 = 1749$. 求 $a^2 + b^2 + c^2 + d^2$ 的所有可能值.
18 数列 $\{a_n\}$ 的每一项都是正整数，$a_1 \leqslant a_2 \leqslant a_3 \leqslant \cdots$ ，且对任意正整数 $k$ ，该数列中恰有 $k$ 项等于 $k$ . 求所有的正整数 $n$ ，使得 $a_1 + a_2 + \cdots + a_n$ 是素数.
19 由正整数组成的数列 $\{a_n\}$ 满足:对任意正整数 $m$ , $n$ ,若 $m \mid n$ $m < n$ ，则 $a_m \mid a_n$ ，且 $a_m < a_n$ . 求 $a_{2000}$ 的最小可能值.
20 设 $p$ 为奇素数，正整数 $m, n$ 满足 $\frac{m}{n} = 1 + \frac{1}{2} + \cdots + \frac{1}{p-1}$ . 证明：$p \mid m$ .
21 设 $a, m, n$ 为正整数，$a > 1$ ，且 $a^m + 1 \mid a^n + 1$ . 证明：$m \mid n$ .
22 证明：对任意正整数 $n$ 及正奇数 $m$ ，都有 $(2^m - 1, 2^n + 1) = 1$ .
23 费马数 $F_n$ 定义为 $F_n = 2^{2^n} + 1$. 证明：对任意两个不同的正整数 $m, n$ ，都有 $(F_n, F_m) = 1$
24 已知正整数 $a, b, c, d$ 的最小公倍数为 $a + b + c + d$. 证明: $abcd$ 是 3 或 5 的倍数.
25 记 $M_n$ 为正整数 $1, 2, \cdots, n$ 的最小公倍数. 求所有的正整数 $n (> 1)$, 使得 $M_n = M_{n-1}$ .
26 设 $a, m, n$ 为正整数，$a > 1$ . 证明：$(a^m - 1, a^n - 1) = a^{(m,n)} - 1$ .
27 设 $a, n$ 为正整数，$a > 1$ ，且 $a^n + 1$ 是素数. 证明：$d\left(a^n - 1\right) \geqslant n$ .
28 对怎样的正整数 $n (> 2)$ ，存在 $n$ 个连续正整数，使得其中最大的数是其余 $n - 1$ 个数的最小公倍数的因数?
29 设正整数 $a, b, m, n$ 满足：$(a, b) = 1, a > 1$ ，且 $a^m + b^m \mid a^n + b^n$ . 证明：$m \mid n$
30 证明：存在 2012 个不同的正整数，使得其中任意两个不同的数 $a, b$ 都满足 $(a - b)^2 \mid ab$.
31 设 $a, b$ 为正整数，且 $(a, b) = 1$ . 证明：对任意正整数 $m$ ，数列

$$a, a + b, a + 2b, \cdots, a + nb, \cdots$$

中，有无穷多个数与 $m$ 互素.
32 已知正整数数对 $(a, b)$ 满足：数 $a^a \cdot b^b$ 在十进制表示下，末尾恰有 98 个零. 求 $ab$ 的最小值.

33 求所有的正整数 $m$, 使得 $m=d(m)^4$ .
34 证明：每一个正整数都可以表示为两个正整数之差，且这两个正整数的素因子个数相同.
35 求所有的正整数 $a,b,c$, 使得 $a^2+1$ 和 $b^2+1$ 都是素数，且满足

$$\left(a^2+1\right)\left(b^2+1\right)=c^2+1$$

36 用 $p(k)$ 表示正整数 $k$ 的最大奇因数. 证明：对任意正整数 $n$ ，都有 $\frac{2}{3}n<\sum_{k=1}^{n}\frac{p(k)}{k}<\frac{2}{3}(n+1)$
37 设 $a,b,c$ 都是大于 1 的正整数. 求代数式 $\frac{a+b+c}{2}-\frac{[a,b]+[b,c]+[c,a]}{a+b+c}$ 的最小可能值.
38 对任意给定的素数 $p$ ，有多少个整数组 $(a,b,c)$ ，使得
(1) $1\leqslant a,b,c\leqslant 2p^2$;
(2) $\frac{[a,c]+[b,c]}{a+b}=\frac{p^2+1}{p^2+2}\cdot c$ .

39 黑板上写着数 $1,2,\cdots,33$ . 每次允许进行下面的操作：从黑板上任取两个满足 $x\mid y$ 的数 $x,y$ ，将它们从黑板上去掉，写上数 $\frac{y}{x}$ . 直至黑板上不存在这样的两个数. 问：黑板上至少剩下多少个数？
40 设 $n$ 是一个正整数. 证明：数 $1+5^n+5^{2n}+5^{3n}+5^{4n}$ 是一个合数.

同余是由大数学家高斯引入的一个概念. 我们可以将它理解为" 余同"，即余数相同. 正如奇数与偶数是依能否被 2 整除而得到的关于整数的分类一样，考虑除以 $m(\geqslant 2)$ 所得余数的不同，可以将整数分为 $m$ 类. 两个属于同一类中的数相对于" 参照物" $m$ 而言，具有" 余数相同" 这个性质. 这种为对比两个整数的性质，引入一个参照物的思想是同余理论的一个基本出发点.

同余是初等数论中的一门语言，是一件艺术品. 它为许多数论问题的表述赋予了统一的, 方便的和本质的形式.