第 1 章　整数的整除与唯一分解

整数性质是初等数论最重要的内容，包括整数的整除和同余等。本章主要介绍整除、带余除法、最大公因子、最小公倍数，以及求最大公因子的算法，并给出整数唯一分解定理。

1.1　整除和带余除法

正整数（如 1, 2, 3,…）、负整数（如– 1, – 2, – 3,…）与零（0）统称为**整数**。

通常，用符号

$$Z = \{0, \pm 1, \pm 2, \pm 3, \cdots\}$$

表示整数集合，零与正整数称为**自然数**。

两个整数的和、差、积仍然是整数，但两个整数相除得到的商未必是整数。为此，我们引入整除、带余除法等概念。

定义 1.1　任意两个整数 a, b，其中 $b \neq 0$，如果存在一个整数 q，使等式

$$a = bq \tag{1.1}$$

成立，我们就说 b **整除** a，或 a 被 b 整除，记为 $b \mid a$。此时，称 b 为 a 的**因子**，a 为 b 的**倍数**。

0 是任何非零整数的倍数，1 是任何整数的因子。

若 $b \mid a$，且 $b \neq 1, b \neq a$，就称 b 是 a 的**真因子**，否则就称 b 为 a 的**平凡因子**。任何非零整数是自身的因子和倍数。式(1.1)中的整数 q 常写成 a/b 或 $\frac{a}{b}$。

如果不存在整数 q 满足式(1.1)，我们就说 b **不整除** a，记为 $b \nmid a$。

设 a, b, c 为整数，根据整除的定义，可以得到以下性质：

① 若 $c \mid b, b \mid a$，则 $c \mid a$（传递性）；

② 若 $b \mid a$，$c \neq 0$，则 $cb \mid ca$；

③ 若 $cb \mid ca$，则 $b \mid a$；

④ 若 $b \mid a$ 且 $a \neq 0$，则 $|b| \leqslant |a|$；

⑤ 若 $b \mid a, a \neq 0$，则 $\frac{a}{b} \mid a$；

⑥ 若 $c \mid a, c \mid b$，则对任意整数 m, n，有 $c \mid ma \pm nb$。

一般地，余数定理如下。

定理 1.1（**带余除法**）　设 a, b 是两个整数，其中 $b > 0$，则存在唯一的整数 q 和 r，使得

$$a = bq + r, 0 \leqslant r < b \tag{1.2}$$

成立。

证明　考虑 b 的整数倍序列

$$\cdots, -3b, -2b, -b, 0, b, 2b, 3b, \cdots$$

在该序列中，整数 a 必位于某两个相邻的整数之间，设该区间为$[qb, (q+1)b)$，即存在整数 q，使得

$$qb \leqslant a < (q+1)b$$

成立。

令 $r = a - qb$，则有

$$a = qb + r, \quad 0 \leqslant r < b$$

进一步，具有上述性质的整数 q, r 是唯一的。

不妨假设存在另一组整数 q_1, r_1，满足

$$a = bq_1 + r_1, \quad 0 \leqslant r_1 < b \tag{1.3}$$

将式(1.3)与式(1.2)相减，得

$$b(q - q_1) = (r_1 - r)$$

所以

$$b \mid q - q_1 \mid = \mid r_1 - r \mid \tag{1.4}$$

等式(1.4)的左边为 b 的倍数，即

$$b \mid q - q_1 \mid = 0 \quad \text{或} \quad b \mid q - q_1 \mid \geqslant b$$

而由于 $0 \leqslant r, r_1 < b$，则等式(1.4)的右边必为

$$0 \leqslant \mid r_1 - r \mid < b$$

因此要使等式(1.4)成立，必须满足

$$q = q_1, \quad r_1 = r$$

式(1.2)称为**带余除法**，或称为**欧几里得除法**。

当 $r = 0$ 时，称 q 为 a 除以 b 的**完全商**；当 $r \neq 0$ 时，称 q 为 a 除以 b 的**不完全商**。通常将 q 通称为商。

r 称为 a 除以 b 得到的**余数**，余数都是非负整数。

为计算商 q，引入下述定义。

定义 1.2 设 x 为实数，小于或等于 x 的最大整数称为 x 的**整数部分**，记为$[x]$；$x - [x]$ 为 x 的**小数部分**。

因此有

$$[x] \leqslant x < [x] + 1$$

整数 a 除以 b 得到的（不完全）商就是$\left[\dfrac{a}{b}\right]$。

事实上，由式(1.2)，得

$$\left[\frac{a}{b}\right] = \left[\frac{qb+r}{b}\right] = \left[q + \frac{r}{b}\right] = q + \left[\frac{r}{b}\right], \ 0 \leqslant r < b$$

因为 $0 \leqslant \dfrac{r}{b} < 1$，所以$\left[\dfrac{r}{b}\right] = 0$。

因此 $q = \left[\dfrac{a}{b}\right]$。

例 1.1　取 $a = 17, b = 5$，则 $q = \left[\frac{17}{5}\right] = [3.4] = 3, r = 17 - 5\times 3 = 2$。

1.2　整数的表示

本节给出正整数的不同进制表示法。对于负整数情况，可通过引入负号，类似得到。

整数通常用十进制数表示，如 $90521 = 9\times 10^4 + 0\times 10^3 + 5\times 10^2 + 2\times 10^1 + 1$。

在计算机领域，整数常用二进制形式、八进制形式或十六进制形式表示。对于任意整数 n 和大于 1 的整数 a，n 可以写成 a 进制形式：

$$n = r_k a^k + r_{k-1}a^{k-1} + \cdots + r_1 a + r_0 \tag{1.5}$$

其中，$r_i \in Z, 0 \leqslant r_i < a, i = 0, 1, \cdots, k$，式(1.5)称为 n 的 ***a* 进制表示**。

n 的 a 进制表示可用带余除法求得。

n 除以 a，设商为 q_0，余数为 r_0，即

$$n = q_0 a + r_0, \quad 0 \leqslant r_0 < a$$

q_0 除以 a，得到

$$q_0 = q_1 a + r_1, \quad 0 \leqslant r_1 < a$$

q_1 除以 a，得到

$$q_1 = q_2 a + r_2, \quad 0 \leqslant r_2 < a$$

以此类推，得到

$$q_i = q_{i+1} a + r_{i+1}, \quad 0 \leqslant r_{i+1} < a, \quad i = 0, 1, 2, \cdots$$

因为 $a > 1$，所以整数序列

$$n > q_0 > q_1 > q_2 > \cdots \geqslant 0$$

为严格递减序列，则一定存在某个 q_t，使 $0 \leqslant q_t < a$，即

$$q_t = 0 \times a + r_{t+1}, \quad 0 \leqslant r_{t+1} < a$$

则

$$\begin{aligned} n &= q_0 a + r_0 \\ &= (q_1 a + r_1)a + r_0 \\ &= q_1 a^2 + r_1 a + r_0 \\ &\quad \cdots \\ &= q_{t-1}a^t + r_{t-1}a^{t-1} + \cdots + r_1 a + r_0 \\ &= (q_t a + r_t)\, a^t + r_{t-1}a^{t-1} + \cdots + r_1 a + r_0 \\ &= r_{t+1}a^{t+1} + r_t a^t + r_{t-1}a^{t-1} + \cdots + r_1 a + r_0 \end{aligned}$$

当 $a = 2$ 时，上述方法可得到任意正整数的二进制表示形式。

例 1.2　将 60801 表示成二进制数形式。

解

$$\begin{aligned} 60801 &= 30400 \times 2 + 1 \quad (r_0 = 1) \\ 30400 &= 15200 \times 2 + 0 \quad (r_1 = 0) \\ 15200 &= 7600 \times 2 + 0 \quad (r_2 = 0) \\ 7600 &= 3800 \times 2 + 0 \quad (r_3 = 0) \end{aligned}$$

$$
\begin{aligned}
3800 &= 1900 \times 2 + 0 \quad (r_4 = 0)\\
1900 &= 950 \times 2 + 0 \quad (r_5 = 0)\\
950 &= 475 \times 2 + 0 \quad (r_6 = 0)\\
475 &= 237 \times 2 + 1 \quad (r_7 = 1)\\
237 &= 118 \times 2 + 1 \quad (r_8 = 1)\\
118 &= 59 \times 2 + 0 \quad (r_9 = 0)\\
59 &= 29 \times 2 + 1 \quad (r_{10} = 1)\\
29 &= 14 \times 2 + 1 \quad (r_{11} = 1)\\
14 &= 7 \times 2 + 0 \quad (r_{12} = 0)\\
7 &= 3 \times 2 + 1 \quad (r_{13} = 1)\\
3 &= 1 \times 2 + 1 \quad (r_{14} = 1)\\
1 &= 0 \times 2 + 1\ (r_{t+1}) \quad (r_{15} = 1)
\end{aligned}
$$

因此

$$60801 = (1110\ 1101\ 1000\ 0001)_2 = 2^{15} + 2^{14} + 2^{13} + 2^{11} + 2^{10} + 2^8 + 2^7 + 1$$

根据十六进制表示法，用 0, 1, 2,…, 9, A, B, C, D, E, F 分别表示 0, 1, 2,…, 9, 10, 11, 12, 13, 14, 15 这 16 个数。也可以反复使用带余除法求得整数的十六进制形式表示。

例 1.3 将 60801 表示成十六进制数。

解

$$
\begin{aligned}
60801 &= 3800 \times 16 + 1 \quad (r_0 = 1)\\
3800 &= 237 \times 16 + 8 \quad (r_1 = 8)\\
237 &= 14 \times 16 + 13 \quad (r_2 = 13)\\
14 &= 0 \times 16 + 14 \quad (r_3 = 14)
\end{aligned}
$$

因此

$$60801 = (\mathrm{E}, \mathrm{D}, 8, 1)_{16} = 14 \times 16^3 + 13 \times 16^2 + 8 \times 16^1 + 1$$

实际上，二进制数与十六进制数有简单的对应关系，例如：

$$60801 = (1110\ 1101\ 1000\ 0001)_2 = [(1110)_2, (1101)_2, (1000)_2, (0001)_2]_{16} = (\mathrm{E}, \mathrm{D}, 8, 1)_{16}$$

表 1.1 列出了十进制数、十六进制数与二进制数三者之间的换算关系。

表 1.1 十进制数、十六进制数和二进制数换算表

十进制数	十六进制数	二进制数	十进制数	十六进制数	二进制数
0	0	0000	8	8	1000
1	1	0001	9	9	1001
2	2	0010	10	A	1010
3	3	0011	11	B	1011
4	4	0100	12	C	1100
5	5	0101	13	D	1101
6	6	0110	14	E	1110
7	7	0111	15	F	1111

根据换算表 1.1，二进制数与十六进制数可以直接相互转换。

例 1.4 十进制数 90521 的二进制数表示为

$$90521 = (10110000110011001)_2$$

则其十六进制数表示为

$$90521 = [(1)_2 \quad (0110)_2 \quad (0001)_2 \quad (1001)_2 \quad (1001)_2]_{16} = (1 \quad 6 \quad 1 \quad 9 \quad 9)_{16}$$

1.3 最大公因子与辗转相除法

本节利用定理 1.1，讨论整数的最大公因子的求法及其性质。

定义 1.3 设 a, b 为两个非零整数，d 为正整数，若

$$d \mid a, d \mid b$$

则 d 称为 a 和 b 的**公因子**。

a 和 b 的公因子中最大的一个称为 a 和 b 的**最大公因子**，记为(a, b)或 $\gcd(a, b)$。若最大公因子$(a, b) = 1$，就称 a 与 b **互素**。

因为 0 可以被任何整数整除，所以任一正整数 a 与 0 的最大公因子就是它自身 a。定义$(0, 0) = 0$。

关于最大公因子，有以下定理。

定理 1.2 设 a, b, c 是任意三个不为零的整数，且

$$a = bq + c, q \text{ 为整数} \tag{1.6}$$

则$(a, b) = (b, c)$。

证明 因为$(a, b) \mid a, (a, b) \mid b$，所以

$$(a, b) \mid c$$

即(a, b)是 b 和 c 的公因子，根据定义 1.3，得

$$(a, b) \leqslant (b, c)$$

同理

$$(b, c) \leqslant (a, b)$$

所以

$$(a, b) = (b, c)$$

接下来讨论最大公因子的求法，即**欧几里得算法**（辗转相除法），并借此给出最大公因子的若干性质。

设 a, b 为两个正整数（$a \geqslant b$），要计算(a, b)，循环使用带余除法（定理 1.1），有下列等式：

$$\begin{cases} a = q_0 b + r_0, & 0 \leqslant r_0 < b \\ b = q_1 r_0 + r_1, & 0 \leqslant r_1 < r_0 \\ r_0 = q_2 r_1 + r_2, & 0 \leqslant r_2 < r_1 \\ \cdots & \\ r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}, & 0 \leqslant r_{n-1} < r_{n-2} \\ r_{n-2} = q_n r_{n-1} + r_n, & 0 \leqslant r_n < r_{n-1} \\ r_{n-1} = q_{n+1} r_n + r_{n+1}, & r_{n+1} = 0 \end{cases} \tag{1.7}$$

事实上，因为整数序列

$$b > r_0 > r_1 > r_2 > \cdots \geqslant 0$$

严格递减，所以必存在某个 n 使得 $r_{n+1} = 0$。

由定理 1.2，得

$$\begin{aligned} r_n &= (0, r_n) \\ &= (r_n, r_{n-1}) \\ &= (r_{n-1}, r_{n-2}) \\ &\cdots \\ &= (r_1, r_0) \\ &= (r_0, b) \\ &= (b, a) \end{aligned}$$

因此，有以下定理。

定理 1.3 任意正整数 a, b，循环使用带余除法，最大公因子(a, b)就是式(1.7)中最后一个不为 0 的余数，即$(a, b) = r_n$。

算法 1.1 用欧几里得算法求 gcd(a, b)。

输入：两个正整数 a, b $(a \geqslant b)$。

输出：gcd(a, b)。

(1) 求 q, r 使得 $a = qb + r, 0 \leqslant r < b$;

(2) 若 $r = 0$，则 $g \leftarrow b$, 输出 g，否则，转(3);

(3) $a \leftarrow b, b \leftarrow r$，转(1)。

例 1.5 求 gcd(156, 79)。

解

$$\begin{aligned} 156 &= 1 \times 79 + 77 \\ 79 &= 1 \times 77 + 2 \\ 77 &= 38 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

故 gcd(156, 79) = 1。

定理 1.4 若整数 $a > b > 0$，则用欧几里得算法求 gcd(a, b)需要不多于 $2\lceil \log_2 a \rceil$次除法运算。

扩展的欧几里得算法。

由算式(1.7)，得

$$\begin{aligned} r_n &= r_{n-2} - q_n r_{n-1} \\ &= r_{n-2} - q_n (r_{n-3} - q_{n-1} r_{n-2}) \\ &= r_{n-2}(1 + q_n q_{n-1}) - q_n r_{n-3} \\ &\cdots \\ &= sa + tb \end{aligned}$$

其中，s, t 为整数。

于是有以下定理。

定理 1.5（最大公因子表示定理） 任意正整数 a, b，存在整数 s, t，使得

$$(a, b) = sa + tb$$

推论 1.1 若 d 是 a 和 b 的公因子，则 $d \mid (a, b)$。

例 1.6 用辗转相除法求(801, 521)及整数 s, t，使得$(801, 521) = 801s + 521t$。

解

$$\begin{aligned}
&801 = 1 \times 521 + 280 && (q_0 = 1, r_0 = 280)\\
&521 = 1 \times 280 + 241 && (q_1 = 1, r_1 = 241)\\
&280 = 1 \times 241 + 39 && (q_2 = 1, r_2 = 39)\\
&241 = 6 \times 39 + 7 && (q_3 = 6, r_3 = 7)\\
&39 = 5 \times 7 + 4 && (q_4 = 5, r_4 = 4)\\
&7 = 1 \times 4 + 3 && (q_5 = 1, r_5 = 3)\\
&4 = 1 \times 3 + 1 && (q_6 = 1, r_6 = 1)\\
&3 = 3 \times 1 + 0
\end{aligned}$$

根据定理 1.3，最后一个不为 0 的余数是 1，所以$(801, 521) = r_6 = 1$。也就是

$$\begin{aligned}
1 &= 4 - 1 \times 3\\
&= 4 - 1 \times (7 - 1 \times 4)\\
&= 2 \times 4 - 1 \times 7\\
&= 2 \times (39 - 5 \times 7) - 1 \times 7\\
&= 2 \times 39 - 11 \times 7\\
&= 2 \times 39 - 11 \times (241 - 6 \times 39)\\
&= 68 \times 39 - 11 \times 241\\
&= 68 \times (280 - 1 \times 241) - 11 \times 241\\
&= 68 \times 280 - 79 \times 241\\
&= 68 \times 280 - 79 \times (521 - 1 \times 280)\\
&= 147 \times 280 - 79 \times 521\\
&= 147 \times (801 - 1 \times 521) - 79 \times 521\\
&= 147 \times 801 - 226 \times 521
\end{aligned}$$

即

$$(801, 521) = 147 \times 801 + (-226) \times 521 = 1$$

定理 1.6 若 $a \mid bc, (a, b) = 1$，则 $a \mid c$。

证明 若 $c = 0$，结论显然成立。

若 $c \neq 0$，由于$(a, b) = 1$，由定理 1.5，存在两个整数 s, t，使

$$sa + tb = 1$$

故

$$sac + tbc = c$$

因为 $a \mid bc$，所以 $a \mid c$。

例 1.7 若 $3 \mid n, 5 \mid n$，则 $15 \mid n$。

证明 由 $3 \mid n$，则存在整数 n_1，使得

$$n = 3n_1$$

又由 $5 \mid n$，即

$$5 \mid 3n_1$$

因为$(5, 3) = 1$，根据定理 1.6，得

$$5 \mid n_1$$

于是存在整数 n_2，使得

$$n_1 = 5n_2$$

即 $n = 3 \cdot 5n_2$。

故 $15 \mid n$。

多个整数的最大公因子的定义如下。

定义 1.4* 设 $a_1, a_2, \cdots, a_n$ 是 n 个整数，d 为正整数，若：

(1) $d \mid a_i$, $i = 1, 2, \cdots, n$;

(2) 对任意正整数 c，若 $c \mid a_i$, $i = 1, 2, \cdots, n$，则 $c \mid d$。

则满足条件(1)的 d 称为 $a_1, a_2, \cdots, a_n$ 的**公因子**；满足条件(1)和(2)的 d 称为 $a_1, a_2, \cdots, a_n$ 的**最大公因子**，记为 $d = (a_1, a_2, \cdots, a_n)$。

当 $n = 2$ 时，由定理 1.5 与推论 1.1，可知定义 1.4 与定义 1.3 等价。

下面的定理说明，计算 n 个整数的最大公因子可以转化为计算一系列的两个整数的最大公因子。

定理 1.7* 设 $a_1, a_2, \cdots, a_n$ 是 n 个整数，令

$$(a_1, a_2) = d_2, (d_2, a_3) = d_3, (d_3, a_4) = d_4, \cdots, (d_{n-2}, a_{n-1}) = d_{n-1}, (d_{n-1}, a_n) = d_n \tag{1.8}$$

则

$$(a_1, a_2, a_3, \cdots, a_n) = d_n$$

且存在整数 $s_1, s_2, \cdots, s_n$，使

$$s_1a_1 + s_2a_2 + \cdots + s_na_n = (a_1, a_2, a_3, \cdots, a_n)$$

成立。

证明 由式(1.8)，得

$$d_i \mid d_{i-1}, \quad i = n, n-1, \cdots, 3$$

且

$$d_n \mid a_n, d_{n-1} \mid a_{n-1}, \cdots, d_3 \mid a_3, d_2 \mid a_2, d_2 \mid a_1$$

所以

$$d_n \mid a_n, d_n \mid a_{n-1}, \cdots, d_n \mid a_2, d_n \mid a_1$$

即 d_n 是整数 $a_1, a_2, a_3, \cdots, a_n$ 的公因子。

假设 c 为 $a_1, a_2, \cdots, a_n$ 的公因子，即

$$c \mid a_i, \quad i = 1, 2, \cdots, n$$

因为 $c \mid a_1, c \mid a_2$，由推论 1.1 得

$$c \mid d_2$$

进一步由 $c \mid a_3$，得

$$c \mid d_3$$

以此类推，最后得

$$c \mid d_n$$

根据定义 1.4，可知 d_n 是 $a_1, a_2, \cdots, a_n$ 的最大公因子。

运用定理 1.5，可证明后一个结论。

由于$(a_1, a_2) = d_2$，因此存在整数 t_1, t_2，使得

$$t_1a_1 + t_2a_2 = d_2$$

由于$(d_2, a_3) = d_3$，因此存在整数 u_1, u_2，使得

$$u_2d_2 + u_3a_3 = d_3$$

即

$$u_2(t_1a_1 + t_2a_2) + u_3a_3 = u_2t_1a_1 + u_2t_2a_2 + u_3a_3 = d_3$$

以此类推，存在整数 $s_1, s_2, \cdots, s_n$，使

$$s_1a_1 + s_2a_2 + \cdots + s_na_n = (a_1, a_2, a_3, \cdots, a_n)$$

例 1.8* 计算 10836, 3744, 7452, 3834, 708 的最大公因子。

解 (1) 计算(10836, 3744)。

$$10836 = 2 \times 3744 + 3348$$
$$3744 = 1 \times 3348 + 396$$
$$3348 = 8 \times 396 + 180$$
$$396 = 2 \times 180 + 36$$
$$180 = 5 \times 36 + 0$$

由定理 1.3，可知最后一个不为 0 的余数就是最大公因子，即(10836, 3744) = 36。

(2) 计算(36, 7452) = 36。

(3) 计算(36, 3834) = 18。

(4) 计算(18, 708) = 6。

所以，10836, 3744, 7452, 3834, 708 的最大公因子是 6。

1.4 最小公倍数

定义 1.5 设 $a_1, a_2, \cdots, a_n$ 是 n 个非零整数，若 m 是这 n 个数中每个数的倍数，即 $a_i \mid m$ $(1 \leqslant i \leqslant n)$，则 m 称为这 n 个数的一个**公倍数**。在 $a_1, a_2, \cdots, a_n$ 的所有公倍数中最小的正整数称为**最小公倍数**，记为$[a_1, a_2, \cdots, a_n]$。

因为乘积$|a_1||a_2|\cdots|a_n|$就是 $a_1, a_2, \cdots, a_n$ 的一个公倍数，所以最小公倍数存在。

由于任何整数都不是 0 的倍数，故讨论最小公倍数时，总假定这些整数均不为 0。

同最大公因子类似，显然有$[a_1, a_2, \cdots, a_n] = [|a_1|, |a_2|, \cdots, |a_n|]$，故只需讨论正整数的最小公倍数。

定义 1.5 也可做如下陈述。

设 $a_1, a_2, \cdots, a_n$ 是 n 个非零整数，m 为正整数，若：

(1) $a_i \mid m$, $i = 1, 2, \cdots, n$；

(2) 对任一正整数 u，若 $a_i \mid u, i = 1, 2, \cdots, n$，则 $m \mid u$。

则满足条件(1)的 m 称为 $a_1, a_2, \cdots, a_n$ 的**公倍数**；满足条件(1)和(2)的 m 称为 $a_1, a_2, \cdots, a_n$ 的**最小公倍数**，记为 $m = [a_1, a_2, \cdots, a_n]$。

当 $n = 2$ 时，定理 1.8 用于求两个整数的最小公倍数。

定理 1.8 设 a, b 是两个正整数，则

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

证明 设 $d = (a, b)$, $a = a_1 d$, $b = b_1 d$。显然，$(a_1, b_1) = 1$。

所以

$$\frac{ab}{(a,b)} = a_1 b_1 d$$

因为

$$a \mid a_1 b_1 d, \quad b \mid a_1 b_1 d$$

由定义 1.5，可知 $a_1 b_1 d$ 是 a 和 b 的公倍数。

下面证明，$a_1 b_1 d$ 是 a 和 b 的最小公倍数。

假设整数 u 满足 $a \mid u, b \mid u$。

由 $a_1 d \mid u$ 得，存在整数 k，使得

$$u = k a_1 d \tag{1.9}$$

由 $b_1 d \mid u$，得

$$b_1 d \mid k a_1 d$$

因此

$$b_1 \mid k a_1$$

因为$(a_1, b_1) = 1$，由定理 1.6，所以

$$b_1 \mid k$$

令 $k = m b_1$，m 为某整数。于是

$$u = m a_1 b_1 d \tag{1.10}$$

因此只要整数 u 满足 $a \mid u, b \mid u$，就有

$$a_1 b_1 d \mid u$$

这就证明了 $a_1 b_1 d$ 是 a 和 b 的最小公倍数，即

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

例 1.9 计算[1946, 2006]。

解 第一步，求(1946, 2006)。

$$2006 = 1 \times 1946 + 60$$
$$1946 = 32 \times 60 + 26$$
$$60 = 2 \times 26 + 8$$
$$26 = 3 \times 8 + 2$$

$$8 = 4 \times 2 + 0$$

所以(1946, 2006) = 2。

第二步，计算

$$[1946, 2006] = \frac{1946 \times 2006}{2} = 1951838$$

求两个以上正整数的最小公倍数，可以转化为一系列求两个正整数的最小公倍数。

设 $a_1, a_2, \cdots, a_n$ 是 n 个正整数，令

$$[a_1, a_2] = m_2, [m_2, a_3] = m_3, \cdots, [m_{n-1}, a_n] = m_n \tag{1.11}$$

有以下结论。

定理 1.9* 若 $a_1, a_2, \cdots, a_n$ 是 n 个正整数，则

$$[a_1, a_2, \cdots, a_n] = m_n$$

证明 由式(1.11)，可得

$$m_i \mid m_{i+1}, i = 2, 3, \cdots, n-1$$

且

$$a_1 \mid m_2, a_2 \mid m_2, a_3 \mid m_3, \cdots, a_n \mid m_n$$

所以

$$a_1 \mid m_n, a_2 \mid m_n, \cdots, a_n \mid m_n$$

即 m_n 是整数 $a_1, a_2, a_3, \cdots, a_n$ 的公倍数。

假设 m 为 $a_1, a_2, \cdots, a_n$ 的公倍数，即

$$a_i \mid m, \quad i = 1, 2, \cdots, n$$

由式(1.11)，可知 $a_1 \mid m, a_2 \mid m$，则

$$m_2 \mid m$$

进一步，由 $a_3 \mid m$，得

$$m_3 \mid m$$

以此类推，最终得

$$m_n \mid m$$

根据定义 1.5，可知 m_n 是 $a_1, a_2, \cdots, a_n$ 的最小公倍数。

定理 1.8 和定理 1.9 给出了两个整数和多个整数的最小公倍数的求法。

例 1.10* 计算 200, 150, 360, 45 的最小公倍数。

解 第一步，根据定理 1.8，求[200, 150]。

$$[200, 150] = \frac{200 \times 150}{(200, 150)} = \frac{200 \times 150}{50} = 600$$

第二步，求[600, 360]。

$$[600, 360] = \frac{600 \times 360}{(600, 360)} = \frac{600 \times 360}{120} = 1800$$

第三步，求[1800, 45]。

$$[1800, 45] = \frac{1800 \times 45}{(1800, 45)} = \frac{1800 \times 45}{45} = 1800$$

所以 1800 即为 200, 150, 360, 45 的最小公倍数。

1.5 整数的唯一分解

一个大于 1 的整数 p，若它的因子只有两个，即 1 和它本身，则称该整数 p 为**素数**；若还包括除 1 和它本身以外的因子，则称该整数为**合数**。1 和 0 既非素数也非合数。

素数与合数是相对立的两个概念，二者是数论中最基础的定义。

本节的主要内容是证明一个大于 1 的整数，若不考虑素数的次序，能唯一地分解成素数（素数幂）的乘积。

定理 1.10 若 p 为素数，a 是任一整数，则 $p \mid a$ 或 $(p, a) = 1$。

证明 因为 $(p, a) \mid p$，根据素数定义，有 $(p, a) = 1$ 或 $(p, a) = p$，后者即 $p \mid a$。

定理 1.11 设 p 为素数，a, b 为整数，若 $p \mid ab$，则 $p \mid a$ 或 $p \mid b$。

证明 由定理 1.10，若 $p \mid a$，得证。

若 $p \nmid a$，则 $(p, a) = 1$。由定理 1.5，可知存在整数 s, t，使得

$$sp + ta = 1$$

所以

$$spb + tab = b$$

由于 $p \mid ab$，因此 $p \mid b$。

定理 1.12（**整数唯一分解定理**） 任意大于 1 的整数可以分解为素数幂形式的乘积

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \tag{1.12}$$

其中，$p_1 < p_2 < \cdots < p_k$ 为素数，$\alpha_1, \alpha_2, \cdots, \alpha_k$ 为正整数。若不考虑素数的次序，这种分解是唯一的。

式(1.12)称为 a 的**标准分解式**。

证明 首先证明标准分解式的存在性。

若 a 是素数，定理显然成立。

若 a 是合数，设 q_1 是 a 的最小真因子，则 q_1 一定是素数（若 q_1 不是素数，则存在 a 的更小的真因子）。

设

$$a = q_1 a_1, \quad 1 < a_1 < a$$

同理，若 a_1 是素数，则分解完毕。

若 a_1 是合数，则 a_1 存在最小的素因子 q_2。

设 $a = q_1 q_2 a_2, 1 \leqslant a_2 < a_1$。

如此进行下去，可得分解形式如下：

$$a = q_1 q_2 q_3 \cdots q_t$$

将相同的素数乘积写成幂形式，即得

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}, \quad p_1 < p_2 < \cdots < p_k, \alpha_i \geqslant 1, i = 1, 2, \cdots, k \tag{1.13}$$

下面证明标准分解式的唯一性。

假设存在 a 的另一组素数分解：

$$a = q_1^{\beta_1} q_2^{\beta_2} \cdots q_t^{\beta_t}, \quad q_1 < q_2 < \cdots < q_t, \beta_i \geqslant 1, i = 1, 2, \cdots, t \tag{1.14}$$

由定理 1.11，可知任一 p_i 必整除某一 q_j，反之 q_j 必整除 p_i，所以 $p_i = q_j$ 且 $k = t$。于是

$$p_1 = q_1, \cdots, p_k = q_k$$

由式(1.13)与式(1.14)得

$$q_1^{\beta_1 - \alpha_1} q_2^{\beta_2} \cdots q_k^{\beta_k} = p_2^{\alpha_2} \cdots p_k^{\alpha_k} \tag{1.15}$$

式(1.15)左边是素数 q_1 的倍数，而式(1.15)右边不是 q_1 的倍数，因此只有

$$\alpha_1 = \beta_1$$

同理可证

$$\alpha_i = \beta_i, \quad i = 1, 2, \cdots, k$$

通常，用符号 $p^{\alpha} \| a$ 表示 $p^{\alpha} | a$，但 $p^{\alpha+1} \nmid a$。如式(1.12)中，$p_1^{\alpha_1} \| a$。

例 1.11 写出 21, 28, 49, 100 的标准分解式。

解 根据定理 1.12，有

$$21 = 3 \times 7$$

$$28 = 2^2 \times 7$$

$$49 = 7^2$$

$$100 = 2^2 \times 5^2$$

唯一分解定理的直接应用是求最大公因子与最小公倍数。

对于式(1.12)有，如果正整数 d 满足 $d | a$，则 d 的标准分解式为

$$d = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}, \quad 0 \leqslant \gamma_i \leqslant \alpha_i, i = 1, 2, \cdots, k \tag{1.16}$$

反之，写成式(1.16)中形式的 d，必有 $d | a$。

定理 1.13 设整数 $a > 0, b > 0$，且

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \quad \alpha_i \geqslant 0, i = 1, 2, \cdots, k$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \quad \beta_i \geqslant 0, i = 1, 2, \cdots, k$$

则

$$(a, b) = p_1^{d_1} p_2^{d_2} \cdots p_k^{d_k}, \quad d_i = \min(\alpha_i, \beta_i), i = 1, 2, \cdots, k \tag{1.17}$$

$$[a, b] = p_1^{m_1} p_2^{m_2} \cdots p_k^{m_k}, \quad m_i = \max(\alpha_i, \beta_i), i = 1, 2, \cdots, k \tag{1.18}$$

其中，符号 $\min(\alpha, \beta)$表示 α, β 中较小的数，符号 $\max(\alpha, \beta)$表示 α, β 中较大的数。

事实上，对任意实数 x, y，显然有

$$x + y = \max(x, y) + \min(x, y)$$

因此

$$[a,b] = \frac{ab}{(a,b)} = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_k^{\max(\alpha_k, \beta_k)}$$

例 1.12　计算 $a = 2^4 \times 3^2 \times 5^3 \times 7^6 \times 11^2$, $b = 3^4 \times 5^2 \times 7^3 \times 11 \times 13^2$ 的最大公因子与最小公倍数。

解　根据定理 1.13，有

$$(a, b) = 3^2 \times 5^2 \times 7^3 \times 11, \quad [a, b] = 2^4 \times 3^4 \times 5^3 \times 7^6 \times 11^2 \times 13^2$$

例 1.13　计算整数 70, 150, 210, 840 的最大公因子和最小公倍数。

解　根据定理 1.12，有

$$70 = 2 \times 5 \times 7$$
$$150 = 2 \times 3 \times 5^2$$
$$210 = 2 \times 3 \times 5 \times 7$$
$$840 = 2^3 \times 3 \times 5 \times 7$$

定理 1.13 可推广到多个整数的情况

$$(70, 150, 210, 840) = 2 \cdot 5 = 10$$
$$[70, 150, 210, 840] = 2^3 \cdot 3 \cdot 5^2 \cdot 7 = 4200$$

若整数 a, b 比较大，通常难以分解，用标准分解式方法求两个数的最大公因子或最小公倍数时，计算量太大。用辗转相除法求最大公因子的优点是，不必考虑整数的分解。

1.6　素数有无穷多

根据 1.5 节的素数定义，2, 3, 5, 7, 11, 13,…都是素数。10 以内的素数有 4 个，100 内的素数有 25 个，1000 以内的素数有 168 个……

关于素数的个数，有以下定理。

定理 1.14　*素数有无穷多个。*

证明　反证法。

假设素数是有限的，设 $p_1 = 2, p_2 = 3, \cdots, p_k$ 是全体素数。

令整数

$$P = p_1 p_2 \cdots p_k + 1$$

因为

$$p_i \nmid P, \ i = 1, 2, \cdots, k$$

所以 P 的任一素因子 q 不等于 $p_i, i = 1, 2, \cdots, k$。于是存在 $p_1, p_2, \cdots, p_k$ 以外的素数，假设错误。

故素数有无穷多个。

定理 1.15（契贝谢夫不等式）*　*设 $x \geqslant 2$，则*

$$\frac{\ln 2}{3} \frac{x}{\ln x} < \pi(x) < 6 \ln 2 \frac{x}{\ln x}$$

以及

$$\frac{1}{6 \ln 2} n \ln n < p_n < \frac{8}{\ln 2} n \ln n$$

其中，p_n 为第 n 个素数。

定理 1.16（**素数定理**） 设 $\pi(x)$表示不大于 x 的所有素数个数，则有

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\ln x}=1 \tag{1.19}$$

根据定理 1.16，可知从不大于 x 的自然数中随机选一个，它是素数的概率大约是 $1/\ln x$。因为 $\lim\limits_{x\to\infty}\dfrac{x/\ln x}{x}=0$，所以 x 越大，素数分布越稀疏。

素数的个数无穷多，但它的分布并不规则，寻找素数是一个比较难的问题，下面讨论埃拉托斯特尼（Eratosthenes）筛法，该方法适于寻找给定界限内的素数序列。

Eratosthenes 筛法利用了这样一条定理。

定理 1.17（**素数判断定理**） 如果 n 不能被不大于 $\sqrt{n}$ 的任何素数整除，则 n 是一个素数。

因此要判断 n 是否为素数，只需判断 n 能否被不大于 $\sqrt{n}$ 的素数整除即可。

例 1.14 求 1～100 以内的所有素数。

分析：只需删除 1 和 1～100 内的所有合数。

根据定理 1.17，可知 1～100 内的所有合数必存在不超过 $\sqrt{100}=10$ 的素因子。

首先，找出 10 以内的所有素数 2, 3, 5, 7。

然后，保留 2, 3, 5, 7，删除 1 以及 2, 3, 5, 7 的所有其他倍数。剩下的数就是 1～100 以内的所有素数，如下所示：

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	(9)	~~10~~
11	~~12~~	13	~~14~~	(15)	~~16~~	17	~~18~~	19	~~20~~
(21)	~~22~~	23	~~24~~	[25]	~~26~~	(27)	~~28~~	29	~~30~~
31	~~32~~	(33)	~~34~~	[35]	~~36~~	37	~~38~~	(39)	~~40~~
41	~~42~~	43	~~44~~	(45)	~~46~~	47	~~48~~	◇49	~~50~~
(51)	~~52~~	53	~~54~~	[55]	~~56~~	(57)	~~58~~	59	~~60~~
61	~~62~~	(63)	~~64~~	[65]	~~66~~	67	~~68~~	(69)	~~70~~
71	~~72~~	73	~~74~~	(75)	~~76~~	◇77	~~78~~	79	~~80~~
(81)	~~82~~	83	~~84~~	[85]	~~86~~	(87)	~~88~~	89	~~90~~
◇91	~~92~~	(93)	~~94~~	[95]	~~96~~	97	~~98~~	(99)	~~100~~

故 100 内的素数共有 25 个，它们是 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97。

在密码算法中往往使用大素数，如二进制数表示的 500 位甚至 1000 位以上的素数。需要使用一些有效的素性检测算法，来判断一个随机整数是否为素数（详见第 5 章）。实际中，判断一个大整数是否为素数要比分解一个大整数容易得多。

素数理论是数论最早的研究课题之一，这方面有若干难题和猜想，至今仍是一个活跃的研究领域。围绕素数存在很多数学问题、数学猜想、数学定理，较为著名的有孪生素数猜想、哥德巴赫猜想等。数学家们通过研究这些难题或猜想，创造了极有价值的数学理论，推动了数学的发展。

1.7 麦什涅数与费马数*

定义 1.6 设 p 是一个素数，形如 2^p-1 的数称为**麦什涅**（Mersenne）**数**，记为 $M_p=2^p-1$。如果 M_p 是素数，就称它为**麦什涅素数**。

麦什涅数不一定都是素数，如 $M_2 = 2^2 - 1 = 3$、$M_3 = 2^3 - 1 = 7$ 是素数，$M_{11} = 2^{11} - 1 = 23 \times 89$ 不是素数。

定理 1.18 *若 $2^n - 1$ 为素数，则 n 必为素数。*

证明 反证法。

假设 $n = kl$ 不是素数，$k > 1$, $l > 1$。于是

$$2^n - 1 = 2^{kl} - 1 = (2^k - 1)(2^{k(l-1)} + \cdots + 2 + 1)$$

而

$$1 < 2^k - 1 < 2^n - 1$$

与题设矛盾，故 n 必为素数。

由定理 1.18，可知形如 $2^n - 1$ 的素数，必为麦什涅素数。

十七世纪，法国数学家麦什涅证明了当 $p = 2, 3, 4, 7, 17, 19, 31$ 时，M_p 是素数。

目前，已知的麦什涅素数有 48 个，它们是：

2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701, 23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787, 1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583, 25964951, 30402457, 32582657（#44）, 37156667, 42643801, 43112609, 57885161（#48）。

现在还不知道在第 44 个麦什涅素数（$M_{25,964,951}$）和第 48 个（$M_{57,885,161}$）之间是否还存在未知的麦什涅素数。

麦什涅素数在代数编码等应用学科中得到了应用。

定义 1.7 *设 n 是自然数，形如 $2^{2^n} + 1$ 的数称为* **费马**（Fermat）**数**，*记为 $F_n = 2^{2^n} + 1$。如果 F_n 是素数，就称它为* **费马素数**。

最小的 5 个费马数为

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$$

它们都是素数。

据此，1640 年法国数学家费马猜想 F_n（$n = 0, 1, 2, \cdots$）均为素数。但在 1732 年，欧拉证明了 $F_5 = 641 \times 6700417$ 是合数。

故费马猜想不正确，不能作为求素数公式。之后，人们又陆续找到了不少反例，如 $F_6 = 274177 \times 67280421310721$ 不是素数。至今，这样的反例共找到了 243 个，却没有找到第 6 个正面的例子。也就是说，目前只知道 $n = 0, 1, 2, 3, 4$ 的情况下，F_n 才是素数。于是有人推测，仅存在有限个费马素数。甚至有人猜想 $n > 4$ 时，费马数全是合数。

几千年来，数学家们一直在寻找这样一个公式，能给出所有素数。但直到现在，谁也未能找到这样的公式，而且未能找到证据，证明这样的公式一定不存在。这样的公式是否存在，成了一个著名的数学难题。

在二进制数的计算机运算中，麦什涅数和费马数可用来提高某些运算的效率。

例如，计算整数 c 除以麦什涅数 M_p 的余数，二进制数表示的 c 容易写成

$$c = c_0 + 2^p c_1 + 2^{2p} c_2 + \cdots + 2^{kp} c_k, \quad 0 \leqslant c_i < 2^p, i = 1, 2, \cdots, k$$

因此

$$c = (2^{kp} - 1)c_k + (2^{kp-1} - 1)c_{k-1} + \cdots + (2^p - 1)c_1 + c_k + c_{k-1} + \cdots + c_1 + c_0$$

c 除以 M_p 的余数与 $c_k + c_{k-1} + \cdots + c_1 + c_0$ 除以 M_p 的余数相同，因此将除法运算转化成加法运算。

若 $c_k + c_{k-1} + \cdots + c_1 + c_0 > M_p$，重复使用上述方法，即可得到 c 除以 M_p 的余数。

关于费马数，可使用类似方法实现快速除法运算。

1.8 素数的著名问题*

关于素数有很多世界级难题，如孪生素数、哥德巴赫猜想等。

孪生素数是指一对素数，两素数之差是 2。如 3 和 5，5 和 7，11 和 13，17 和 19，…，101 和 103，…，10016957 和 10016959 等都是孪生素数。

即使是大素数，也有可能是孪生素数。通过穷举计算发现，在小于 10^{15} 的 29 844 570 422 669 个素数中，有 1 177 209 242 304 对孪生素数，占了 3.94%。

孪生素数猜想：存在无穷多个素数 p，使得 $p + 2$ 也是素数。

孪生素数猜想是数论中著名的未解决问题。这个猜想由希尔伯特在 1900 年巴黎国际数学家大会的报告上第 8 个问题中提出，可以描述为“存在无穷多对孪生素数”。该问题尚未解决。

至 2011 年底，发现的最大的孪生素数是

$$3756801695685\times2^{666669} - 1,\ 3756801695685\times2^{666669} + 1$$

这对素数中的每个都长达 200700 位。

孪生素数方面迄今最好的结果是 1966 年由已故的中国数学家陈景润利用筛法（sieve method）取得的。陈景润证明了：存在无穷多个素数 p，使得 $p + 2$ 要么是素数，要么是两个素数的乘积。

孪生素数猜想可以弱化为“能不能找到一个正数，使得有无穷多对素数之差小于这个给定的正数”的问题，在孪生素数猜想中，这个正数就是 2。华人数学家张益唐找到的正数是“70000000”。

2013 年 5 月 14 日，《自然》（Nature）杂志在线报道，美国新罕布什尔大学的华人数学家张益唐证明了“存在无穷多个之差小于 70000000 的素数对”，这一研究被认为在孪生素数猜想这一数论问题上取得了重大突破。

哥德巴赫猜想（也称为“1+1”问题）是数论中存在最久的未解问题之一，也是希尔伯特第八个问题中的一个子问题。这个猜想最早出现在 1742 年普鲁士数学家哥德巴赫写给瑞士数学家欧拉的通信中。哥德巴赫猜想可以陈述为：

“任一大于 2 的偶数，都可表示成两个素数之和。”

例如，$4 = 2 + 2$, $8 = 3 + 5$, $10 = 5 + 5$, $12 = 5 + 7$, $14 = 7 + 7$, $16 = 3 + 13$, $18 = 5 + 13$,…

目前，最好的结果是陈景润在 1973 年发表的陈氏定理（也称为“1+2”定理），即“任一充分大的偶数都可以表示成二个素数的和，或是一个素数与两个素数积的和。”用通俗的话说就是，“大偶数 = 素数 + 素数”，或“大偶数 = 素数 + 素数 × 素数”。

数学中的猜想和难题，有的在提出后不久便被解决，有的尚未解决，数学家们在研究这些猜想和难题的过程中，推动了数学的发展。

习 题 1

1．设 $n = 3219$，证明：n 被 3 整除，但不被 5, 7 整除。

2．证明：存在整数 k，使得 $5 \mid 2k + 1$，并尝试给出整数 k 的一般形式。

3．证明：$3 \nmid 3k + 2$，其中 k 为整数。

4．设正整数 n 的 p 进制表示为 $n = a_0 + a_1 p + \cdots + a_k p^k$，证明：$a_i = \left[\frac{n}{p^i}\right] - p\left[\frac{n}{p^{i+1}}\right]$，（$0 \leqslant i \leqslant k$）。

5．将十进制数 7535 分别表示成二进制数和十六进制数。

6．将二进制数$(1\ 1100\ 0100\ 1110)_2$, $(100\ 1010\ 1011\ 0011)_2$ 转化为十六进制数和十进制数。

7．将十六进制数$(ABCDEF)_{16}$, $(EFA0D57B)_{16}$ 分别转化为二进制数和十进制数。

8．使用扩展的欧几里得算法计算整数 s, t，使得 $sa + tb = (a, b)$：

(1) (489, 357)；　(2) (187, 221)；　(3) (6188, 4709)。

9．将下列各组整数的最大公因子分别表示为整系数的线性组合。

(1) (2, 7, 11)；　(2) (6, 21, 27)；　(3) (42, 63, 161)。

10．设 $n \in Z$，证明：$6 \mid n(n + 1)(n + 2)$。

11．证明：每个奇数的平方具有 $8k + 1$ 形式。

12．证明：

(1) 形如 $3k + 1$ 的奇数一定是形如 $6h + 1$ 的整数；

(2) 形如 $3k - 1$ 的奇数一定是形如 $6h - 1$ 的整数。

13．如果 $a \in Z$，证明：$3 \mid a^3 - a$。

14．如果 $3 \nmid n$，证明：$3 \mid n^2 - 1$。

15．设 $a, b \in Z$，令 $d = (a, b)$，且 $a = da_1, b = db_1$，证明：$(a_1, b_1) = 1$。

16．设 $a, b \in Z, a \neq 0$，证明：$(a, a + b) \mid b$。

17．设 $a, b \in Z$，证明：$(a, b) = (a, ka + b)$，其中 k 为任意整数。

18．设 $u, v, n \in Z$，如果$(u, v) = 1$，且 $u \mid n, v \mid n$，证明：$uv \mid n$。

19．设 a, b 为整数，d 为正整数，证明：$(ad, bd) = d(a, b)$。

20．设 $a, b, c \in Z$，$(a, b) = 1$，证明：$(a, bc) = (a, c)$。

21．设 $u, v \in Z$，$(u, v) = 1$，证明：$(u + v, u - v) = 1$ 或 2。

22．设 $m, n \in Z^+$，整数 $a > 1$，证明：$(a^m - 1, a^n - 1) = a^{(m, n)} - 1$。

23．设 $n \in Z^+$，证明：$1 + \frac{1}{2} + \frac{1}{3} + \ldots + \frac{1}{n}$ 不是整数。

24．求 388 与 572 的最小公倍数。

25．设 $a, b \in Z$，$m \in Z^+$，证明：$(ma, mb) = m(a, b)$，$[ma, mb] = m[a, b]$。

26．设 $a_1, a_2, \cdots, a_n \in Z$，证明：$(a_1, a_2, \cdots, a_n) = ((a_1, \cdots, a_s), (a_{s+1}, \cdots, a_n))$。

27．设 $a_1, a_2, \cdots, a_n \in Z$，证明：$[a_1, a_2, \cdots, a_n] = [[a_1, \cdots, a_s], [a_{s+1}, \cdots, a_n]]$。

28．证明：$\sqrt{2}$ 是无理数，即证明：不存在有理数 $r = a/b$ 使得 $r^2 = 2$。

29．设 $m \in Z$，证明：$\sqrt[n]{m}$ 是有理数当且仅当 m 是某个整数的 n 次方。

30．证明：$\log_2 10, \log_3 11, \log_{10} 15$ 都是无理数。

31．是否存在这样的整数 a, b, c，使得 $a \mid bc$，但 $a \nmid b, a \nmid c$？

32．设 $a, b \in Z$，$n \in Z^+$，$(a, b) = 1$，证明：$(a^n, b^n) = 1$。

33．设 $a, b \in Z$，$n \in Z^+$，$a \mid b$，证明：$a^n \mid b^n$。

34．设合数 $n\in Z^+$，p 是素数，若 $p>n^{1/3}$，证明：n/p 是素数。

35．设 $n\in Z^+$，证明：n 可唯一地写成 $n=ab^k$，其中，a, b, k 为正整数，不存在整数 $d>1$ 使得 $d^k \mid a$。

36．写出下列各数的素因子分解：

(1) 16；　(2) 28；　(3) 300；　(4) 3740。

37．设 n 个正整数 $a_1, a_2,\cdots, a_n$ 的标准分解式为

$$\begin{cases} a_1 = p_1^{\alpha_{11}} p_2^{\alpha_{12}} \cdots p_k^{\alpha_{1k}} \\ a_2 = p_1^{\alpha_{21}} p_2^{\alpha_{22}} \cdots p_k^{\alpha_{2k}} \\ \cdots \\ a_n = p_1^{\alpha_{n1}} p_2^{\alpha_{n2}} \cdots p_k^{\alpha_{nk}} \end{cases}$$

其中，$p_1<p_2<\cdots<p_k$, $0\leqslant \alpha_{ij}$ $(i=1,2,\cdots,n, j=1,2,\cdots,k)$。证明：

(1) $(a_1, a_2,\cdots, a_n)=p_1^{d_1} p_2^{d_2}\cdots p_k^{d_k}$，$d_j=\min(\alpha_{1j}, \alpha_{2j},\cdots, \alpha_{nj},), j=1,2,\cdots,k$。

(2) $[a_1, a_2,\cdots, a_n]=p_1^{m_1} p_2^{m_2}\cdots p_k^{m_k}$，$m_j=\max(\alpha_{1j}, \alpha_{2j},\cdots, \alpha_{nj},), j=1,2,\cdots,k$。

38．已知下列各数的因数分解，写出其最大公因子和最小公倍数：

(1) $2^3\cdot3\cdot5^4\cdot11^3\cdot13$, $2^2\cdot3^3\cdot5^2\cdot7\cdot11^3\cdot13^2\cdot17$；

(2) $2\cdot3\cdot5\cdot7\cdot11$, $13\cdot17\cdot19\cdot23$；

(3) $2\cdot3\cdot5\cdot7\cdot11\cdot17^3$, $2\cdot3^3\cdot5^2\cdot7^2\cdot13^3\cdot17^3$, $2^2\cdot3^2\cdot5^3\cdot7^4\cdot13^2\cdot17^3\cdot19$；

(4) $29^2\cdot47^3\cdot79^5\cdot89^2\cdot101^3$, $23^4 41^2 47^5 97^9 101$, $23^4 29^2\cdot41\cdot47^2\cdot79^4\cdot89^3\cdot101^4$。

39．设 $n\in Z^+$，有标准因数分解

$$a=p_1^{\alpha_1} p_2^{\alpha_2}\ldots p_k^{\alpha_k},\quad \alpha_i\geqslant 1 \quad (i=1,2,\cdots,k)$$

证明：n 的因数个数为 $d(n)=(1+\alpha_1)\cdots(1+\alpha_k)$。

40．设 a, b 为正整数，p 为素数，用 $\mathrm{ind}_p(a)$表示 a 的标准分解式中所含 p 的幂次。证明：

$$\mathrm{ind}_p(a+b)\geqslant \min\left(\mathrm{ind}_p(a), \mathrm{ind}_p(b)\right)$$

且当 $\mathrm{ind}_p(a)\neq \mathrm{ind}_p(b)$时，等号成立。

41．设 $a, b\in Z^+$，则$(a, b) \mid [a, b]$，什么条件下有$(a, b)=[a, b]$?

42．证明：奇素数一定能表示成两个平方数之差。

43．设 $k\in Z^+$，证明：形如 $4k-1, 6k-1$ 的素数有无穷多。

44．运用 Eratosthenes 筛法求出 200 以内的所有素数。

45．证明：$641 \mid F_5$，从而第 5 个费马数是合数。

46．设 $p_1=2<p_2<\cdots<p_n<\cdots$是递增的素数列，证明：$p_n<2^{2^{n-1}}$。

47．已知费马数的形式为 $F_n=2^{2^n}+1, n\in Z^+$，证明：不同的费马数两两互素。由此推出素数有无穷多。

48．求 $5x+7y=100$ 的整数解。

49．如果 a^n-1 是素数，证明：$a=2$ 且 n 为素数。

50．如果 a^n+1 是素数，证明：a 为偶数且 n 为 2 的幂。

51．设 $a, b, c\in Z$，a, b 不全为零，则不定方程 $ax+by=c$ 有解的充要条件是$(a, b) \mid c$；如果有解 x_0, y_0，则方程的所有解可表示为

$$x=x_0-k\frac{b}{(a,b)},\quad y=y_0-k\frac{a}{(a,b)}$$

其中，$k=0, \pm1, \pm2,\cdots$。

52．证明：不定方程 $x^4+y^4=z^2$ 没有正整数解。