

第2章 整除

从本章起, 我们主要介绍数论理论. 数论主要是关于整数性质的理论, 在数学理论体系中占有独特的地位, 它的许多问题在概念上很容易理解, 但是解决起来却非常困难. 数学家高斯曾经说过“数学是科学的女王, 数论是数学的女王”, 这代表了许多年以来人们将数论看作纯粹的理论数学而不是应用数学的普遍观点. 然而, 正是这个数学领域却在当今的互联网络时代中发挥了巨大作用, 它与编码理论、密码学等信息科学关系密切.

数论理论的重要基础是整除. 在整数集合中, 整除是一种重要的二元关系, 相关的概念和性质包括素数、公因数和公倍数、辗转相除、算术基本定理等, 这些概念和性质又是整数集合中另一种重要的二元关系——同余关系的基础. 本章将对整数整除的相关概念和性质作详细的介绍.

2.1 整除与带余除法

我们通常用 \mathbf{N} 表示正整数(自然数)集合, 即 $\mathbf{N} = \{1, 2, 3, \dots\}$, 用 \mathbf{Z} 表示整数集合, 即 $\mathbf{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$. 我们知道, 两个整数的和、差、积仍然是整数, 但如果我们用一个非零整数去除另一个整数, 所得的商则不一定为整数.

定义 2.1.1 设 $a, b \in \mathbf{Z}$, $b \neq 0$. 如果存在 $q \in \mathbf{Z}$ 使得 $a = qb$, 那么就称 a 可被 b 整除或者 b 整除 a , 记为 $b|a$, 且称 a 是 b 的倍数, b 是 a 的因子(也可称为约数或除数). 若 a 不能被 b 整除, 则记为 $b \nmid a$.

需要注意的是, 符号 $b|a$ 本身就包含了条件 $b \neq 0$, 不过 $a = 0$ 是允许的. 同时, 我们需要记住这个定义的关键在于整除关系是通过整数的乘法定义的, 而不是通过除法定义的.

定义 2.1.2 若 b 为 a 的因子, 且 $b \neq \pm 1$, $b \neq \pm a$, 则称 b 为 a 的真因子.

例如 2 和 7 是 14 的真因子, 而 1 和 14 虽然是 14 的因子, 但不是真因子.

定理 2.1.1 设 $a, b \in \mathbf{Z}$, 则有

- (1) $b|a \Leftrightarrow -b|a \Leftrightarrow b|-a \Leftrightarrow |b| \mid |a|$;
- (2) 设 $a \neq 0$, 如果 $b|a$, 那么 $|b| \leq |a|$.

证明 (1) 可由以下各式两两等价推出: $a = qb$, $a = (-q)(-b)$, $-a = (-q)b$, $|a| = |q| |b|$, 其中 $q \in \mathbf{Z}$.

(2) 由(1)知 $|a| = |q| |b|$. 当 $a \neq 0$ 时, $|q| \geq 1$. 定理得证.

定理 2.1.2 设 $a, b, c \in \mathbf{Z}$,

- (1) 若 $b|a$ 且 $c|b$, 则 $c|a$;
- (2) 若 $b|a$, 则 $b|ac$;
- (3) 设 $c \neq 0$, 则 $b|a \Leftrightarrow bc|ac$;
- (4) $b|a$ 且 $b|c \Leftrightarrow$ 对任意的 $m, n \in \mathbf{Z}$ 有 $b|ma+nc$.

证明 (1) 因为 $b|a$ 且 $c|b$, 则存在整数 q_1 和 q_2 使得 $a = q_1b$, $b = q_2c$, 从而推出 $a = (q_1 q_2)c$.

(2) 因为 $b|a$, 则存在整数 q 使得 $a = qb$, 从而 $ac = (qc)b$.

(3) 由于 $c \neq 0$, 故 $a = qb$ 与 $ac = q(bc)$ 等价, 其中 q 为整数.

(4) 因为 $b|a$ 且 $b|c$, 则存在整数 q_1 和 q_2 , 使得 $a = q_1b$, $c = q_2b$, 从而

$$ma + nc = mq_1b + nq_2b = (mq_1 + nq_2)b.$$

必要性得证. 取 $m = 1, n = 0$ 及 $m = 0, n = 1$ 就可推出充分性. 我们可以将 $ma + nc (m, n \in \mathbf{Z})$ 形式的整数称为整数 a 和 c 的**整系数线性组合**. 尽管在读者看来这一条也像前面几条那样很直观, 然而, 下面的一些证明中会反复应用整除的这个性质, 即如果一个整数整除另外两个整数, 那么必然整除它们的任意整系数线性组合.

例 2.1.1 证明: 若 $b|a$ 且 $a|b$, 则 $b = \pm a$.

证明 因为 $b|a$ 且 $a|b$, 则存在整数 q_1 和 q_2 使得

$$a = q_1b, \quad b = q_2a,$$

可得 $a = q_1q_2a$. 由于 $a \neq 0$, 所以 $q_1q_2 = 1$, $q_2 = \pm 1$. 从而 $b = \pm a$.

例 2.1.2 设 $a = 2t - 1$. 若 $a|2n$, 则 $a|n$.

证明 由 $a|2n$ 知 $a|2tn$, 又 $a|an$, 根据定理 2.1.2(4), 则 $a|2tn - an$. 由 $a = 2t - 1$ 知 $2tn - an = 2tn - 2tn + n = n$. 代入即得 $a|n$.

例 2.1.3 设 a, b 是两个给定的非零整数, 且有整数 x, y , 使得 $ax + by = 1$. 证明: 若 $a|n$ 且 $b|n$, 则 $ab|n$.

证明 由

$$n = n(ax + by) = (na)x + (nb)y,$$

又 $ab|na, ab|nb$, 根据定理 2.1.2(4)即得.

上面几个定理的证明中只需要利用整数的加法、减法和乘法的性质, 这三个整数运算的结果都没有超出整数的范围, 一旦我们考虑整数的除法, 我们就需要用到整数的另一个性质, 即所谓的良序原理.

良序原理 每一个由非负整数组成的非空集合 S 必定含有一个最小元素, 也就是说, S 中存在一个元素 a , 对任意 $b \in S$, 都有 $a \leq b$ 成立.

很显然, 良序原理符合我们对整数的直观感受和日常使用要求, 但是这个原理是无法证明的, 只能作为公理写出, 它是我们证明下面一些定理的关键基础和依据.

定理 2.1.3 设 a 和 b 为任意整数, $b > 0$, 则存在唯一的一对整数 q 和 r , 使

$$a = qb + r, \quad 0 \leq r < b. \quad (2.1.1)$$

其中 a 称为**被除数**, q 称为**商**, r 称为**余数**(或非负最小剩余).

证明 先证明存在性. 令集合

$$S = \{a - xb \mid x \in \mathbf{Z} \text{ 且 } 0 \leq a - xb\}$$

这个集合是非负整数的集合, 且不是空集: 因为 $b \geq 1$, 所以 $|a|b \geq |a|$, 那么 $a - (-|a|)b = a + |a|b \geq a + |a| \geq 0$. 即当 $x = -|a|$ 时, $a - xb \in S$. 根据良序原理, S 含有一个最小的元素 r , 由集合 S 的定义可知, 存在整数 q 满足

$$r = a - qb, \quad r \geq 0.$$

我们也能证明 $r < b$: 因为如果 $r < b$ 不成立, 则 $r \geq b$, 那么

$$a - (q+1)b = (a - qb) - b = r - b \geq 0.$$

所以 $a - (q+1)b \in S$. 但是 $a - (q+1)b = (a - qb) - b = r - b < r$, 这与 r 是 S 的最小元素相矛盾, 于是 $r < b$, 存在性得证.

下面来证明唯一性. 假设存在另一对整数 q_1 和 r_1 满足(2.1.1)式, 即

$$a = q_1b + r_1, \quad 0 \leq r_1 < b. \quad (2.1.2)$$

设 $r < r_1$, 则 $0 < r_1 - r < b$. 将(2.1.1)和(2.1.2)两式相减, 得 $(q - q_1)b = r_1 - r$, 故 $b|(r_1 - r)$. 这个结果与 $0 < r_1 - r < b$ 矛盾(定理 2.1.1(2)). 同理如果设 $r_1 < r$, 也会导出矛盾. 所以 $r = r_1$, 进而 $q = q_1$. 证毕.

这个定理也被称作带余除法. 如果 $b < 0$: 由于 $-b > 0$, 这个定理意味着存在整数 q_1 与 r

使得 $a = q_1(-b) + r$, $0 \leq r < -b$. 此时, 令 $q = -q_1$, 我们就能得到这个定理的推广, 只要 $b \neq 0$, 就存在唯一的一对整数 q 和 r , 使 $a = qb + r$, $0 \leq r < |b|$.

显然, $b|a$ 的充要条件是 $r = 0$. 注意当 a 是负数时的余数可以不同 (但两个余数之和为 $|b|$). 比较一个简单的例子中的两个余数的不同, 如果用 7 去除 60 和 -60, 得到 $60 = 7 \times 8 + 4$ 和 $-60 = 7 \times (-9) + 3$.

定义 2.1.3 设 $a, q, r \in \mathbf{Z}$, 满足 $a = 2q + r$, $0 \leq r < 2$. 若 $r = 0$, 称 a 为**偶数**; 若 $r = 1$, 称 a 为**奇数**.

定义 2.1.4 一个大于 1 的整数 p , 若仅以 1 和自身 p 为其正因子, 则称 p 为**素数** (或**质数**). 除 1 以外非素的正整数则称为**合数** (或**复合数**).

素数具有许多特殊而又美妙的性质, 并且在数论科学的发展中起着十分重要的作用. 历史上的许多数学家都不禁为之倾倒. 下面介绍几个关于素数的基本定理.

定理 2.1.4 素数有无穷多个.

证明 用反证法. 假定只有有限个素数 p_1, p_2, \dots, p_k , 考虑 $a = p_1 p_2 \cdots p_k + 1$. 由于 a 是合数, 所以它必有素因子, 不妨假定这个素因子为 p_j ($1 \leq j \leq k$), 显然 $p_j | a$. 因为

$$a - p_1 p_2 \cdots p_k = 1,$$

又 $p_j | (p_1 p_2 \cdots p_k)$, 故 $p_j | 1$. 但是素数 $p_j \geq 2$, 所以 $p_j | 1$ 是不可能的. 因此推出矛盾, 假设错误. 定理得证.

定理 2.1.5 对任意正整数 n , 存在素数 p 满足 $n < p \leq n! + 1$.

证明 考虑正整数 $a = n! + 1$. 如果 a 是素数, 则可取 $p = a$. 如果 a 是合数, 则必有某个素因子 p . 先假定 $p \leq n$, 那么必有 $p | n!$, 所以 $p | (a - n!)$, 即 $p | 1$, 出现了矛盾, 因此 $p > n$. 定理得证.

定理 2.1.6 如果整数 $n \geq 2$, 那么在 $n! + 2$ 与 $n! + n$ 之间必没有素数.

证明 由于 $n!$ 是从 1 到 n 的所有整数的连乘积, 所以有

$$2 | (n! + 2), 3 | (n! + 3), \dots, n | (n! + n).$$

证毕.

定理 2.1.7 若 n 为合数, 则 n 必有素因子 p 满足 $p \leq \sqrt{n}$.

证明 不妨设 p 为 n 的最小素因子. 如果有 $n = rs$, 其中 r 和 s 均为 n 的真因子, 那么 $p \leq r$ 且 $p \leq s$. 所以 $p^2 \leq rs = n$, 即 $p \leq \sqrt{n}$.

定理 2.1.7 给出了一种寻找素数的有效方法. 为了求出不超过给定正整数 $x (> 1)$ 的所有素数, 只要把从 2 到 x 的所有合数都删去即可. 因为不超过 x 的合数 a 必有一个素因子 $p \leq \sqrt{a} \leq \sqrt{x}$, 所以只要先求出 \sqrt{x} 以内的全部素数 $\{p_i, 1 \leq i \leq k\}$ (其中 k 为 \sqrt{x} 以内的素数个数), 然后把不超过 x 的 p_i 的倍数 (p_i 本身除外) 全部删去, 剩下的就正好是不超过 x 的全部素数. 这种寻找素数的方法称为 Eratosthenes 筛法. 下面是一个具体应用的实例.

例 2.1.4 求出不超过 64 的所有素数.

解 先求出不超过 $\sqrt{64} = 8$ 的全部素数, 依次为 2, 3, 5, 7. 然后从 2 到 64 的所有整数中依次删去除了 2, 3, 5, 7 以外的 2 的倍数, 3 的倍数, 5 的倍数和 7 的倍数, 剩下的即为所求. 具体过程如下所示.

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

可以看出, 没有删去的数是

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61.

它们就是不超过 64 的所有素数.

习题 2.1

A 组

1. 证明若 $2|n, 5|n, 7|n$, 那么 $70|n$.
2. 利用 Eratosthenes 筛法求出 500 内的全部素数.
3. 证明任意三个连续的正整数的乘积都被 6 整除.
4. 证明每个奇数的平方都具有 $8k+1$ 的形式.

B 组

1. 证明若 $m-p|mn+pq$, 则 $m-p|mq+np$.
2. 证明若 a 是整数, 则 $a^3 - a$ 能被 3 整除.
3. 对于任意给定的正整数 k , 必有 k 个连续的正整数都是合数.
4. 编写程序求 1000000 内的所有素数.

2.2 最大公因子与辗转相除法

定义 2.2.1 设 a_1, a_2, \dots, a_n 是 n 个不全为零的整数. 若整数 d 是它们之中每一个数的因子, 那么 d 就称为 a_1, a_2, \dots, a_n 的一个公因子. 在整数 a_1, a_2, \dots, a_n 的所有公因子中最大的一个称为最大公因子, 记作 (a_1, a_2, \dots, a_n) 或者 $\gcd(a_1, a_2, \dots, a_n)$. 特别地, 若 $(a_1, a_2, \dots, a_n) = 1$, 我们称 a_1, a_2, \dots, a_n 互素 (或互质).

例如, 12 和 -18 的公因子为 $\{\pm 1, \pm 2, \pm 3, \pm 6\}$, 它们的最大公因子 $(12, -18) = 6$. 而 $(12, -18, 35) = 1$, 于是我们说 12, -18 和 35 这三个整数是互素的. 需要注意的是, 符号 (a_1, a_2, \dots, a_n) 本身就包含了条件 a_1, a_2, \dots, a_n 不全为零.

定理 2.2.1 设 a, b, c 是任意三个不全为零的整数, 且 $a = bq + c$, 其中 q 是整数, 则 $(a, b) = (b, c)$.

证明 因为 $(a, b)|a$, $(a, b)|b$, 又 $c = a - bq$, 所以 $(a, b)|c$, 即 (a, b) 是 b 和 c 的公因子, 因而 $(a, b) \leq (b, c)$. 同理可证 $(b, c) \leq (a, b)$, 于是 $(a, b) = (b, c)$. 结合带余除法, 我们可以得到这样的结论, 被除数与除数的最大公因子等于除数与余数的最大公因子.

由最大公因子的定义, 我们不难得到 $(a_1, a_2, \dots, a_n) = (|a_1|, |a_2|, \dots, |a_n|)$. 另外, 欲求一组不全为零的整数的最大公因子, 只要求出其中全体非零整数的最大公因子即可, 因为它们是相等的. 于是, 我们先讨论两个正整数的最大公因子的求法. 当然, 我们可以运用最大公因子的定义, 先分别求出这两个数的所有因子, 再从中挑出它们的最大公因子. 在这两个数比较小的情况下, 这种方法是可行的, 但若这两个数相对较大, 那么分解其因子是十分困难的, 我们只能另想办法. 下面我们介绍一种“辗转相除法”, 它可以很好地解决求两个正整数的最大公因子的问题, 而且就目前来讲, 这也是能在计算机上实现的解决此问题最好的算法. 这个算法也被称作“欧几里德除法”.

任给两个正整数 a 和 b , 不妨设 $a \geq b$, 由定理 2.1.3, 有下列等式:

$$\begin{aligned} a &= bq_1 + r_1, \quad 0 < r_1 < b, \\ b &= r_1q_2 + r_2, \quad 0 < r_2 < r_1, \\ &\vdots \end{aligned}$$

$$\begin{aligned} r_{n-2} &= r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1}, \\ r_{n-1} &= r_n q_{n+1} + r_{n+1}, \quad r_{n+1} = 0. \end{aligned} \quad (2.2.1)$$

因为 $b > r_1 > r_2 > \cdots > r_n > r_{n+1} = 0$, 所以经过有限步后, 总可以得到一个余数是零, 即(2.2.1)式中 $r_{n+1} = 0$.

定理 2.2.2 若任给两个正整数 a 和 b , 则 (a, b) 就是(2.2.1)式中最后一个不等于零的余数, 即 $(a, b) = r_n$.

证明 由定理 2.2.1 可知

$$r_n = (0, r_n) = (r_n, r_{n-1}) = \cdots = (r_2, r_1) = (r_1, b) = (a, b).$$

定理得证.

定理 2.2.2 实际上给出了计算两个正整数最大公约数的算法, 即著名的欧几里德算法.

算法 2.2.1 欧几里德算法求 r_0 和 r_1 的最大公约数

输入: 正整数 r_0 和 $r_1, r_0 > r_1$

输出: (r_0, r_1)

```
i = 1
do
    i = i + 1
    r_i = r_{i-2} % r_{i-1}
while( r_i != 0)
return r_{i-1}
```

定理 2.2.3 对任意两个正整数 a 和 b , 一定存在两个整数 m, n , 使得

$$(a, b) = ma + nb.$$

即 (a, b) 是 a 和 b 的整系数线性组合.

证明 由(2.2.1)式可知

$$r_n = r_{n-2} - r_{n-1}q_n,$$

即 r_n 是 r_{n-2} 和 r_{n-1} 的线性组合, 将 $r_{n-1} = r_{n-3} - r_{n-2}q_{n-1}$ 代入得 $r_n = r_{n-2}(1 + q_n q_{n-1}) - r_{n-3}q_n$, 即 r_n 是 r_{n-3} 和 r_{n-2} 的线性组合, 再将 $r_{n-2} = r_{n-4} - r_{n-3}q_{n-2}$ 代入, 那么 r_n 也是 r_{n-4} 和 r_{n-3} 的线性组合, 如此继续下去, 直到将(2.2.1)式的最开始的两个式子代入完毕, 最终可得 r_n 也是 a 和 b 的线性组合, 即存在两个整数 m, n , 使得 $r_n = ma + nb$. 又根据定理 2.1.9 知 $(a, b) = r_n$, 定理得证.

显然, 定理 2.2.3 中 a 和 b 的取值可推广到全部整数范围.

例 2.2.1 设 $a = 8\,656$, $b = -7\,780$, 求 (a, b) 和整数 m, n , 使 $ma + nb = (a, b)$.

解 $(a, b) = (8\,656, -7\,780) = (8\,656, 7\,780)$. 运用辗转相除法, 有

$$\begin{aligned} 8\,656 &= 7\,780 \times 1 + 876, \\ 7\,780 &= 876 \times 8 + 772, \\ 876 &= 772 \times 1 + 104, \\ 772 &= 104 \times 7 + 44, \\ 104 &= 44 \times 2 + 16, \\ 44 &= 16 \times 2 + 12, \\ 16 &= 12 \times 1 + 4, \\ 12 &= 4 \times 3 + 0. \end{aligned}$$

因此, $(a, b) = 4$. 再由

$$\begin{aligned} 4 &= 16 - 12 \times 1 \\ &= 16 - (44 - 16 \times 2) \\ &= 16 \times 3 - 44 \end{aligned}$$

初始步骤

回代步骤

整理步骤

$$\begin{aligned}
&= (104 - 44 \times 2) \times 3 - 44 && \text{回代步骤} \\
&= 104 \times 3 - 44 \times 7 && \text{整理步骤} \\
&= 104 \times 3 - (772 - 104 \times 7) \times 7 && \text{回代步骤} \\
&= 104 \times 52 - 772 \times 7 && \text{整理步骤} \\
&= (876 - 772 \times 1) \times 52 - 772 \times 7 && \text{回代步骤} \\
&= 876 \times 52 - 772 \times 59 && \text{整理步骤} \\
&= 876 \times 52 - (7780 - 876 \times 8) \times 59 && \text{回代步骤} \\
&= 876 \times 524 - 7780 \times 59 && \text{整理步骤} \\
&= (8656 - 7780 \times 1) \times 524 - 7780 \times 59 && \text{回代步骤} \\
&= 8656 \times 524 - 7780 \times 583 && \text{整理步骤} \\
&= 8656 \times 524 + (-7780) \times 583, && \text{规范步骤}
\end{aligned}$$

因此, 整数 $m = 524$, $n = 583$, 使 $ma + nb = (a, b)$.

从上面这个例子中, 我们看到在求整数 m, n 时, 初始步骤是将 $r_{n-2} = r_{n-1}q_n + r_n$ 写成 $r_n = r_{n-2} - r_{n-1}q_n$ 的形式, 然后需要交替进行回代步骤和整理步骤直到 a 和 b 出现在等式的右边, 最后的规范步骤是为了得到具有正确的正负号的 m, n , 需要注意的是该步骤的关键在于, 中间的符号必须为 ‘+’.

定理 2.2.4 设整数 a, b, c 满足 $c|a$ 且 $c|b$, 则 $c|(a, b)$.

证明 由定理 2.2.3 可知, 存在两个整数 m, n , 使得

$$(a, b) = ma + nb.$$

因为 $c|a$ 且 $c|b$, 故 $c|ma + nb$, 即 $c|(a, b)$ (即公因子整除最大公因子).

定理 2.2.5 设有整数 a, b, c , 其中 $c > 0$, 则 $(ac, bc) = (a, b)c$.

证明 由定理 2.2.3 可知, 存在两个整数 m, n 使得

$$(a, b) = ma + nb.$$

将等式左右两端同乘 c , 得

$$(a, b)c = m(ac) + n(bc).$$

因为 $(ac, bc) | m(ac) + n(bc)$, 所以 $(ac, bc) | (a, b)c$.

又显然有 $(a, b)c | ac$, $(a, b)c | bc$, 由定理 2.2.4 可知 $(a, b)c | (ac, bc)$.

因此, $(ac, bc) = (a, b)c$, 定理得证.

例 2.2.2 设 $a = 16 \times 2350$, $b = 27 \times 2350$, 求 (a, b) .

解 $(a, b) = (16, 27) \times 2350 = 1 \times 2350 = 2350$.

例 2.2.3 证明: 若整数 a, b, d 满足 $d|a$, $d|b$, 则

$$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a, b)}{|d|}.$$

特别地, $\left(\frac{a}{(a, b)}, \frac{b}{(a, b)}\right) = 1$.

证明 因为 $d|a$, $d|b$, 则由定理 2.2.5 我们有

$$\begin{aligned}
(a, b) &= \left(\frac{a}{|d|} \cdot |d|, \frac{b}{|d|} \cdot |d|\right) \\
&= \left(\frac{a}{|d|}, \frac{b}{|d|}\right) |d| \\
&= \left(\frac{a}{d}, \frac{b}{d}\right) |d|,
\end{aligned}$$

所以 $\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a, b)}{|d|}$. 特别地, 当 $d = (a, b)$ 时, 有

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

定理 2.2.6 整数 a, b 互素的充分必要条件是存在整数 x, y , 使得

$$xa + yb = 1.$$

证明 由互素的定义及定理 2.2.3, 必要性显然得证.

再证充分性. 不妨设 $d = (a, b)$, 则 $d|a$ 且 $d|b$. 若存在整数 x, y 使得

$$xa + yb = 1,$$

则有 $d|xa+yb$, 即 $d|1$, 所以 $d=1$, a, b 互素. 证毕.

定理 2.2.7 设有整数 a, b, c , 若 $a|bc$ 且 $(a, b) = 1$, 则 $a|c$.

证明 若 $c=0$, 结论显然成立. 下面不妨假定 $c \neq 0$.

因为 $(a, b) = 1$, 由定理 2.2.6 可知, 存在整数 m, n 使得

$$ma + nb = 1.$$

将等式左右两端同乘 c , 得

$$mac + nbc = c.$$

因为 $a|ac$, $a|bc$, 所以 $a|mac + nbc$, 即 $a|c$. 定理得证.

以上我们讨论了两个整数的最大公因子的求解问题, 那么对于两个以上的整数, 我们如何才能求出其最大公因子呢?

定理 2.2.8 设 a_1, a_2, \dots, a_n 是 n 个整数, 其中 $a_1 \neq 0$. 令

$$(a_1, a_2) = d_2, (d_2, a_3) = d_3, \dots, (d_{n-1}, a_n) = d_n,$$

则

$$(a_1, a_2, \dots, a_n) = d_n.$$

证明 由 $d_n|a_n$, $d_n|d_{n-1}$, $d_{n-1}|a_{n-1}$, $d_{n-1}|d_{n-2}$, 可知 $d_n|a_{n-1}$, $d_n|d_{n-2}$. 依此类推, 可得

$$d_n|a_n, \quad d_n|a_{n-1}, \quad \dots, \quad d_n|a_1,$$

故 d_n 是 a_1, a_2, \dots, a_n 的公因子.

不妨设 d 为 a_1, a_2, \dots, a_n 的任意公因子. 因为 $d|a_1, d|a_2$, 则由定理 2.2.4 我们有 $d|d_2$, 又 $d|a_3$, 则 $d|d_3$. 依此类推, 可得 $d|d_n$. 故 $d \leq d_n$.

根据最大公因子的定义, 可知

$$(a_1, a_2, \dots, a_n) = d_n.$$

证毕.

例 2.2.4 计算 $(90, 30, 114, 42, 81)$.

解 因为

$$(90, 30) = 30,$$

$$(30, 114) = 6,$$

$$(6, 42) = 6,$$

$$(6, 81) = 3,$$

所以 $(90, 30, 114, 42, 81) = 3$.

定义 2.2.2 设 a_1, a_2, \dots, a_n 是 n 个整数, 若 m 是这 n 个数中每一个数的倍数, 则 m 就称为这 n 个数的一个**公倍数**. 在 a_1, a_2, \dots, a_n 的所有公倍数中最小的正整数称为**最小公倍数**, 记作 $[a_1, a_2, \dots, a_n]$ 或者 $\text{lcm}(a_1, a_2, \dots, a_n)$.

例如, 12 和 -18 的公倍数为 $\{\pm 36, \pm 72, \dots\}$, 它们的最小公倍数 $[12, -18] = 36$. 由于任何正整数都不是零的倍数, 故讨论整数的最小公倍数时, 总假定这些整数都不为零. 类似于最大公因子, 我们有 $[a_1, a_2, \dots, a_n] = [|a_1|, |a_2|, \dots, |a_n|]$. 于是, 我们先讨论两个正整数的最小公倍数的求法.

定理 2.2.9 设 a 和 b 为任意两个互素正整数, 则其乘积即为最小公倍数.

证明 设 m 是 a, b 的任一公倍数, 即 $a|m, b|m$. 则有 $m = ak$, 即 $b|ak$, 其中 k 为正整数. 又 $(a, b) = 1$, 则 $b|k$. 于是存在正整数 t 使 $k = bt$, $m = abt$, 即 $ab|m$, 故 $ab \leq m$. 由于 ab 显然是 a, b 的公倍数, 且不大于 a, b 的任一公倍数 m , 所以它就是最小公倍数. 定理得证.

定理 2.2.10 设 a 和 b 为任意正整数, 则

(1) 若 m 是 a, b 的任一公倍数, 则 $[a, b]|m$;

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

证明 设正整数 x, y 满足 $m = ax = by$, 令 $a = a_1(a, b)$, $b = b_1(a, b)$, 则 $a_1x = b_1y$. 因为 $(a_1, b_1) = 1$, 所以 $b_1|x$, 即存在正整数 t 使 $x = b_1t$. 于是, 我们有

$$m = ax = ab_1t = \frac{ab}{(a, b)}t.$$

根据定理 2.2.9, 有 $[a_1, b_1] = a_1b_1$, 即

$$\left[\frac{a}{(a, b)}, \frac{b}{(a, b)}\right] = \frac{ab}{(a, b)^2}.$$

将等式两端同乘 (a, b) , 得

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

于是(2)得证. 所以有 $m = [a, b]t$, 即 $[a, b]|m$, (1)也得证.

现在我们开始讨论两个以上整数的最小公倍数, 给出下面的定理.

定理 2.2.11 设 a_1, a_2, \dots, a_n 是 n 个整数, 令

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

则

$$[a_1, a_2, \dots, a_n] = m_n.$$

证明 因为 $m_i|m_{i+1}$ ($i = 2, 3, \dots, n-1$), 且 $a_1|m_2$, $a_i|m_i$ ($i = 2, 3, \dots, n$), 所以 m_n 是 a_1, a_2, \dots, a_n 的公倍数. 又设 m 是 a_1, a_2, \dots, a_n 的任一公倍数, 则由 $a_1|m, a_2|m$, 可知 $m_2|m$, 又 $a_3|m$, 可得 $m_3|m$. 依此类推, 最后得 $m_n|m$, 因此 $m_n \leq m$. 所以 $m_n = [a_1, a_2, \dots, a_n]$.

例 2.2.5 计算 $[90, 30, 114, 42, 81]$.

解 因为

$$[90, 30] = \frac{90 \times 30}{(90, 30)} = \frac{90 \times 30}{30} = 90,$$

$$[90, 114] = \frac{90 \times 114}{(90, 114)} = \frac{90 \times 114}{6} = 1710,$$

$$[1710, 42] = \frac{1710 \times 42}{(1710, 42)} = \frac{1710 \times 42}{6} = 11970,$$

$$[11970, 81] = \frac{11970 \times 81}{(11970, 81)} = \frac{11970 \times 81}{9} = 107730,$$

所以 $[90, 30, 114, 42, 81] = 107730$.

定理 2.2.12 设 a_1, a_2, \dots, a_n 是 n 个正整数, 如果 $a_1|m, a_2|m, \dots, a_n|m$, 则

$$[a_1, a_2, \dots, a_n]|m.$$

证明 对 n 用数学归纳法.

当 $n = 2$ 时, 由定理 2.2.10 可知.

假设 $n = k$ ($2 < k < n$) 时, 命题成立, 即 $m_k|m$, 其中 $m_k = [a_1, a_2, \dots, a_k]$.

当 $n = k + 1$ 时, 由

$$[m_k, a_{k+1}] = [a_1, a_2, \cdots, a_k, a_{k+1}],$$

可得 $[a_1, a_2, \cdots, a_{k+1}] | m$. 于是定理得证.

习题 2.2

A 组

1. 求如下整数对的最大公因子:
(1) (55, 85); (2) (202, 282); (3) (666, 1414); (4) (20785, 44350).
2. 证明若整数 a, b 满足 $(a, b) = 1$, 那么 $(a+b, a-b) = 1$ 或 2.
3. 证明若 m, n 为正整数, a 是大于 1 的整数. 则有 $(a^m-1, a^n-1) = a^{(m,n)}-1$.
4. 求如下整数对的最小公倍数:
(1) (231, 732); (2) (-871, 728).

B 组

1. 证明 $12 | n^4 + 2n^3 + 11n^2 + 10n, n \in \mathbf{Z}$.
2. 设 $3 | a^2 + b^2$, 证明 $3 | a$ 且 $3 | b$.
3. 设 n, k 是正整数, 证明 n^k 与 n^{k+4} 的个位数字相同.
4. 证明对于任何整数 n, m , 等式 $n^2 + (n+1)^2 = m^2 + 2$ 不可能成立.
5. 设 a 是自然数, 问 $a^4 - 3a^2 + 9$ 是素数还是合数?
6. 证明对于任意给定的 n 个整数, 必可以从中找出若干个数作和, 使得这个和能被 n 整除.
7. 编写程序计算整数 a, b 的最大公因子.

2.3 算术基本定理

我们前面讨论了一些有关素数和整数分解的问题, 知道任意一个大于 1 的整数都至少有两个正因子, 即 1 和它本身, 且必有素因子. 那么是否每个整数一定可以唯一表示成若干素数的乘积呢? 接下去的部分就讨论这个问题.

定理 2.3.1 设 p 为素数且 $p | ab$, 则 $p | a$ 或 $p | b$.

证明 若 a 能被 p 整除, 则定理显然得证. 若 a 不能被 p 整除, 则 $(a, p) = 1$, 可知存在整数 m, n , 使得

$$ma + np = 1,$$

所以

$$mab + npb = b.$$

由于 $p | ab$, 所以 $p | b$. 定理得证.

推论 设 p 为素数, 若 $p | a_1 a_2 \cdots a_n$, 其中 a_1, a_2, \cdots, a_n 是 n 个整数, 则 $p | a_1, p | a_2, \cdots, p | a_n$ 至少有一个成立.

证明 用数学归纳法.

当 $n = 2$ 时, 根据定理 2.3.1, 显然成立.

假设 $n-1$ 时命题成立, 即若 $p | a_1 a_2 \cdots a_{n-1}$, 则 $p | a_1, p | a_2, \cdots, p | a_{n-1}$ 至少有一个成立.

对于 n , 由于 $p | (a_1 a_2 \cdots a_{n-1}) a_n$, 所以 $p | a_1 a_2 \cdots a_{n-1}$ 或 $p | a_n$. 再根据归纳假设, 可知 $p | a_1, p | a_2, \cdots, p | a_{n-1}, p | a_n$ 至少有一个成立. 命题得证.

上面的定理及其推论非常重要,因为它们给出了素数最重要的特点之一. 如果 p 不是素数, 上面的结果不一定成立. 例如, $6 \nmid 12$ 且 $12 = 3 \times 4$, 但是 $6 \nmid 3$ 且 $6 \nmid 4$.

定理 2.3.2 设 a_1, a_2, \dots, a_n, c 是整数, 如果 $(a_i, c) = 1, 1 \leq i \leq n$, 则 $(a_1 a_2 \cdots a_n, c) = 1$.

证明 用反证法. 假设存在大于 1 的整数 m 满足 $(a_1 a_2 \cdots a_n, c) = m$, 则必存在素数 p , 使 $p \mid m$, 于是 $p \mid a_1 a_2 \cdots a_n$ 且 $p \mid c$. 由上面的推论, 可知 $p \mid a_1, p \mid a_2, \dots, p \mid a_n$ 至少有一个成立, 则 $(a_i, c) = p$ 至少有一个成立. 这与命题中 $(a_i, c) = 1$ 矛盾, 于是假设不成立. 定理得证.

定理 2.3.3 任一大于 1 的整数都可以表示成素数的乘积, 且在不考虑乘积顺序的情况下, 该表达式是唯一的. 即

$$n = p_1 p_2 \cdots p_s, \quad p_1 \leq p_2 \leq \cdots \leq p_s, \quad (2.3.1)$$

其中 p_1, p_2, \dots, p_s 是素数, 并且若

$$n = q_1 q_2 \cdots q_t, \quad q_1 \leq q_2 \leq \cdots \leq q_t, \quad (2.3.2)$$

其中 q_1, q_2, \dots, q_t 是素数, 则 $s = t, p_i = q_i \quad (i = 1, 2, \dots, s)$.

证明 首先, 用数学归纳法证明(2.3.1)式成立.

当 $n = 2$ 时, (2.3.1)式显然成立.

假设对于一切大于 1 且小于 n 的正整数, (2.3.1)式都成立.

对于正整数 n , 若 n 是素数, 则(2.3.1)式对 n 成立.

若 n 是合数, 则存在正整数 b, c 满足条件

$$n = bc, \quad 1 < b \leq c < n,$$

由归纳法假设, b 和 c 分别能表示成素数的乘积, 故 n 能表示成素数的乘积, 即(2.3.1)式成立.

下面证明唯一性.

假设对 n 同时有(2.3.1)和(2.3.2)两式成立, 则

$$p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t. \quad (2.3.3)$$

由定理 2.3.1 可知, $\exists p_k, q_j$ 使得 $p_1 \mid q_j, q_1 \mid p_k$, 但由于 p_k 和 q_j 均为素数, 故 $p_1 = q_j, q_1 = p_k$. 又 $p_1 \leq p_k, q_1 \leq q_j$, 故同时有 $p_1 \leq q_1, q_1 \leq p_1$, 因此 $p_1 = q_1$, 由(2.3.3)式得

$$p_2 \cdots p_s = q_2 \cdots q_t.$$

同理可得 $p_2 = q_2, p_3 = q_3$, 依此类推, 可知 $s = t$ 时, $p_s = q_s$. 唯一性得证.

以上定理被称为**算术基本定理**, 也叫作整数的**唯一分解定理**, 它反映了整数的本质. 将(2.3.2)式中相同的素数乘积写成素数幂的形式, 可得以下推论.

推论 任一大于 1 的整数都能够唯一地表示成

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \quad \alpha_i > 0, \quad i = 1, 2, \dots, s, \quad (2.3.4)$$

其中 $p_i < p_j \quad (i < j)$ 是素数.

(2.3.4)式称为 n 的**标准分解式**.

定理 2.3.4 设 n 是大于 1 的任一整数, 其标准分解式由(2.3.4)式给出, 那么 d 是 n 的正因子的充要条件是

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}, \quad \alpha_i \geq \beta_i \geq 0, \quad i = 1, 2, \dots, s. \quad (2.3.5)$$

证明 先证充分性. 若(2.3.5)式成立, 则存在正整数

$$c = p_1^{\alpha_1 - \beta_1} p_2^{\alpha_2 - \beta_2} \cdots p_s^{\alpha_s - \beta_s},$$

显然有 $n = cd$, 所以 $d|n$.

再证必要性.

设 $d|n$, 且 d 有素因子分解式

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}, \beta_i \geq 0, i = 1, 2, \cdots, s,$$

则必有

$$\alpha_i \geq \beta_i, i = 1, 2, \cdots, s.$$

否则, 至少存在一个 i 满足 $1 \leq i \leq s$, 使 $\alpha_i < \beta_i$. 不妨设 $\alpha_1 < \beta_1$. 由于 $d|n$ 及 $p_1^{\beta_1} | d$, 所以

$$p_1^{\beta_1} | p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}.$$

又由 $p_1^{\alpha_1} > 0$, 可得

$$p_1^{\beta_1 - \alpha_1} | p_2^{\alpha_2} \cdots p_s^{\alpha_s}.$$

根据 2.3.1 的推论, 可知存在 k 满足 $2 \leq k \leq s$, 使 $p_1 | p_k$, 这是不可能的. 于是必要性亦得证.

由以上定理可知, 只要我们知道了正整数 n 的标准分解式, 那么其所有的正因子也都可以知道了, 且可以由(2.3.5)式给出. 我们不难得出以下定理.

定理 2.3.5 设正整数 n 的标准分解式为

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \alpha_i > 0, i = 1, 2, \cdots, s,$$

$\tau(n)$ 表示 n 的所有正因子的个数, 则

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

例 2.3.1 计算 360 的所有正因子的个数.

解 因为 $360 = 2^3 \times 3^2 \times 5$, 所以

$$\tau(360) = (3+1)(2+1)(1+1) = 24.$$

再根据最大公因子和最小公倍数的定义, 我们显然可以得到如下结论.

定理 2.3.6 设 a, b 为两个正整数, 其素因子分解式分别为

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \alpha_i \geq 0, i = 1, 2, \cdots, s,$$

$$b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}, \beta_i \geq 0, i = 1, 2, \cdots, s,$$

那么

$$(a, b) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s}, \gamma_i = \min(\alpha_i, \beta_i), i = 1, 2, \cdots, s,$$

$$[a, b] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_s^{\delta_s}, \delta_i = \max(\alpha_i, \beta_i), i = 1, 2, \cdots, s.$$

对于任意的整数 α, β , 显然有

$$\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta,$$

由此可得

$$(a, b)[a, b] = ab,$$

由于 (a, b) 不可能为零, 所以这个结果和定理 2.2.10 中已经证明过的结果相同.

例 2.3.2 计算整数 90, 30, 114, 42, 81 的最大公因子与最小公倍数.

解 先写出这些整数的标准分解式, 即

$$\begin{aligned}
90 &= 2 \times 3^2 \times 5, \\
30 &= 2 \times 3 \times 5, \\
114 &= 2 \times 3 \times 19, \\
42 &= 2 \times 3 \times 7, \\
81 &= 3^4,
\end{aligned}$$

于是

$$\begin{aligned}
(90, 30) &= 2 \times 3 \times 5 = 30, \\
(30, 114) &= 2 \times 3 = 6, \\
(6, 42) &= 2 \times 3 = 6, \\
(6, 81) &= 3,
\end{aligned}$$

所以整数 90, 30, 114, 42, 81 的最大公因子是 3.

由于

$$\begin{aligned}
[90, 30] &= 2 \times 3^2 \times 5 = 90, \\
[90, 114] &= 2 \times 3^2 \times 5 \times 19 = 1\ 710, \\
[1\ 710, 42] &= 2 \times 3^2 \times 5 \times 7 \times 19 = 11\ 970, \\
[11\ 970, 81] &= 2 \times 3^4 \times 5 \times 7 \times 19 = 107\ 730,
\end{aligned}$$

所以整数 90, 30, 114, 42, 81 的最小公倍数是 107 730.

例 2.3.3 证明对于正整数 a, b, c , 有 $(a, [b, c]) = [(a, b), (a, c)]$.

证明 由于其素因子分解式可分别写为

$$\begin{aligned}
a &= p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \\
b &= p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}, \\
c &= p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_s^{\gamma_s},
\end{aligned}$$

其中 $\alpha_i, \beta_i, \gamma_i \geq 0, i = 1, 2, \cdots, s$, 则

$$(a, [b, c]) = p_1^{\eta_1} p_2^{\eta_2} \cdots p_s^{\eta_s},$$

其中 $\eta_i = \min(\alpha_i, \max(\beta_i, \gamma_i)), i = 1, 2, \cdots, s$.

$$[(a, b), (a, c)] = p_1^{\tau_1} p_2^{\tau_2} \cdots p_s^{\tau_s},$$

其中 $\tau_i = \max(\min(\alpha_i, \beta_i), \min(\alpha_i, \gamma_i)), i = 1, 2, \cdots, s$.

不难验证, 对于 $i = 1, 2, \cdots, s$, 无论 $\alpha_i, \beta_i, \gamma_i$ 有怎样的大小关系, $\eta_i = \tau_i$ 总是成立的. 于是命题得证.

例 2.3.4 设 a, b 是两个正整数, 则存在整数 c, d , 满足 $c|a, d|b$, 使得

$$cd = [a, b], \quad (c, d) = 1.$$

证明 设 a, b 可写成如下的因子分解式

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \quad b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s},$$

其中当 $i = 1, \cdots, t$ 时, $\alpha_i \geq \beta_i \geq 0$; 当 $i = t + 1, \cdots, s$ 时, $\beta_i > \alpha_i \geq 0$.

取

$$c = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_t^{\alpha_t}, \quad d = p_{t+1}^{\beta_{t+1}} \cdots p_s^{\beta_s}$$

即为所求.

习题 2.3

A 组

1. 求以下整数的标准分解式

(1) 36; (2) 69; (3) 200; (4) 289.

2. 求以下整数的标准分解式

(1) 625; (2) 2154; (3) 2838; (4) 3288.

B 组

1. 写出 22345680 的标准分解式.

2. 证明在 $1, 2, \dots, 2n$ 中任取 $n+1$ 数, 其中至少有一个能被另一个整除.

3. 证明 $1 + \frac{1}{2} + \dots + \frac{1}{n}$ ($n \geq 2$) 不是整数.

4. 设 a, b 是正整数. 证明存在 a_1, a_2, b_1, b_2 , 使得 $a = a_1 a_2, b = b_1 b_2, (a_2, b_2) = 1$, 并且 $[a, b] = a_2 b_2$.

5. 证明 n 的标准分解式中次数都是偶数当且仅当 n 是完全平方数.

2.4^{*} 完全数、梅森素数和费马素数

由于素数在数论中占有最重要的地位, 数学家们一直希望找到能够描述素数的简单规律, 尽管到目前为止这样的规律还没有找到, 但是在这个过程中提出的一些问题, 尤其是关于具有某些特定形式的素数的问题及相关概念, 对密码学等学科具有比较重要的应用价值.

定义 2.4.1 若正整数 n 的所有正因子之和等于 $2n$, 则 n 称为**完全数**.

今后我们以 $\sigma(n)$ 表示正整数 n 的所有正因子之和, 于是, 若 n 为完全数, 则有 $\sigma(n) = 2n$.

例 2.4.1 判断 6 和 28 是否为完全数.

解 由于 6 的所有正因子为 1, 2, 3, 6, 则

$$\sigma(6) = 1 + 2 + 3 + 6 = 2 \times 6,$$

所以 6 是完全数. 又 28 的所有正因子为 1, 2, 4, 7, 14, 28, 则

$$\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2 \times 28,$$

所以 28 也是完全数.

定理 2.4.1 若正整数 n 的标准分解式为

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s},$$

则

$$\sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_s^{\alpha_s+1} - 1}{p_s - 1}.$$

¹ 书中, 标记*的章节为扩展内容, 读者可根据具体情况选择阅读。

证明 由定理 2.3.4 可知, n 的所有因子可表示为

$$p_1^{x_1} p_2^{x_2} \cdots p_s^{x_s}, \quad 0 \leq x_i \leq \alpha_i, \quad i = 1, 2, \cdots, s,$$

故

$$\begin{aligned} \sigma(n) &= \sum_{x_1=0}^{\alpha_1} \cdots \sum_{x_s=0}^{\alpha_s} p_1^{x_1} \cdots p_s^{x_s} \\ &= \sum_{x_1=0}^{\alpha_1} p_1^{x_1} \cdots \sum_{x_s=0}^{\alpha_s} p_s^{x_s} \\ &= \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdots \frac{p_s^{\alpha_s+1} - 1}{p_s - 1} \end{aligned}$$

证毕.

定理 2.4.2 若 $2^n - 1$ 为素数, 则 $2^{n-1}(2^n - 1)$ 为偶完全数, 且无其他偶完全数存在.

证明 令 $p = 2^n - 1$, 则

$$2^{n-1}(2^n - 1) = 2^{n-1}p,$$

于是

$$\sigma(2^{n-1}p) = \frac{2^n - 1}{2 - 1} \frac{p^2 - 1}{p - 1} = p(p + 1) = 2^n p.$$

所以 $2^{n-1}(2^n - 1)$ 为完全数. 又显然有 $n \geq 2$, 故 $2^{n-1}(2^n - 1)$ 为偶完全数.

若 a 为一偶完全数, 不妨令 $a = 2^{n-1}q$, 其中 $n \geq 2$, q 为奇数, 则有

$$\sigma(a) = 2a = 2^n q = \frac{2^n - 1}{2 - 1} \cdot \sigma(q),$$

故

$$\sigma(q) = \frac{2^n q}{2^n - 1} = q + \frac{q}{2^n - 1},$$

可知 $2^{n-1} | q$, 则 q 和 $\frac{q}{2^n - 1}$ 均为 q 的因子, 又 $\sigma(q)$ 为 q 的所有正因子之和, 故 q 只有两个正因子, 由整数的唯一分解定理和素数定义知 q 为素数, 且

$$\frac{q}{2^n - 1} = 1.$$

所以 $q = 2^n - 1$, 即 $a = 2^{n-1}(2^n - 1)$. 证毕.

于是, 寻找偶完全数的问题就可化为寻找形如 $2^n - 1$ 的素数的问题. 而“ $2^n - 1$ 是素数”与“ n 是素数”之间是否存在着一定的联系呢? 当 n 等于 2, 3, 5, 7 时, $2^n - 1$ 毫无疑问是素数, 但 $2^{11} - 1 = 2047 = 23 \times 89$. 由此可见, 若 n 是素数, $2^n - 1$ 不一定是素数.

定理 2.4.3 若 $2^n - 1$ 为素数, 则 n 必为素数.

证明 对于 $n > 1$, 假设 n 为合数, 即 $n = bc$, 其中 b, c 均为大于 1 的整数, 则 $2^{b-1} | 2^n - 1$, 所以 $2^n - 1$ 为合数, 于是定理得证.

定义 2.4.2 设 p 是一个素数, 形如 $2^p - 1$ 的数叫作**梅森数**, 记为 $M_p = 2^p - 1$. 当 M_p 为素数时, 则称其为**梅森素数**.

梅森 (Marin Mersenne, 1588—1648) 是法国的修道士, 也是一位数学家. 当时, 他无证明地提出, 对不大于 257 的素数 p , 当且仅当 $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ 时, M_p 为素数. 当然, 他的这个结论是有错误的. 其中, M_{67} 和 M_{257} 是合数, 而 M_{61} , M_{89} , M_{107} 也应该是素数, 但这些结果的全部给出却是在三百多年以后的 1947 年. 至今已经知道有 40 个梅森素数, 下面列出了它们所对应的 40 个 p .

2	3	5	7	13	17	19	31
61	89	107	127	521	607	1 279	2 203
2 281	3 217	4 253	4 423	9 689	9 941	11 213	19 937
21 701	23 209	44 497	86 243	110 503	132 049	216 091	756 839
859 433	1 257 787	1 398 269	2 976 221	3 021 377			
6 972 593	13 466 917	20 996 011					

我们知道, 每发现一个梅森素数, 就可以相应地得到一个偶完全数. 是否存在无穷多个 p 使 M_p 为素数, 进而得到无穷多个偶完全数, 这是至今尚未解决的数论难题. 那么是否存在奇完全数呢? 尽管几百年来许多数学家对此问题进行了大量的研究, 但至今仍未解决.

定理 2.4.4 若 $2^m + 1$ 为素数, 则 $m = 2^n$.

证明 假设 m 有一个奇因子 q , 令 $m = qr$, 则

$$2^{qr} + 1 = (2^r)^q + 1 = (2^r + 1)(2^{r(q-1)} - \cdots + 1),$$

又 $1 < 2^r + 1 < 2^{qr} + 1$, 故 $2^m + 1$ 非素数, 与已知条件矛盾. 所以 m 没有奇因子, 定理得证.

定义 2.4.3 若 n 为非负整数, 则称 $F_n = 2^{2^n} + 1$ 为**费马数**. 当 F_n 为素数时, 则称其为**费马素数**.

最前 5 个费马数分别为 $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$, 它们都是素数. 据此, 1640 年, 法国数学家费马 (Pierre de Fermat, 1601—1665) 猜想凡 F_n 皆为素数. 1732 年, 瑞士数学家欧拉 (Leonhard Euler, 1707—1783) 发现 $F_5 = 641 \times 6\,700\,417$, 故费马猜想并不正确, 并且到目前为止, 也只发现了这 5 个费马素数, 因此有人推测仅存在有限个费马素数.

定理 2.4.5 任给两个费马数 F_a, F_b , $a \neq b$, 则 F_a, F_b 互素.

证明 不妨设 $a > b \geq 0$, $a = b + c$, $c > 0$, 存在正整数 n , 满足 $n | F_b$ 且 $n | F_{b+c}$, 显然 n 必为奇数. 令 $t = 2^{2^b}$, 则有

$$\frac{F_{b+c} - 2}{F_b} = \frac{2^{2^{b+c}} - 1}{2^{2^b} + 1} = \frac{t^{2^c} - 1}{t + 1} = t^{2^c-1} - t^{2^c-2} + \cdots - 1,$$

故 $F_b | F_{b+c} - 2$, 又由 $n | F_b$ 且 $n | F_{b+c}$, 可知 $n | 2$. 因为 n 是奇数, 所以 $n = 1$, 即 F_a, F_b 互素.