第 1 章 整除

本章我们主要介绍数论理论中的整除. 数论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, 在当今的网络时代中发挥了巨大作用, 它与编码理论、密码学等信息科学领域关系密切.

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、公因数与公倍数、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. 本章我们将对整数整除的相关概念和性质进行详细的介绍. 另外, 我们还会讨论连分数及其在公钥密码 RSA 攻击中的应用. 最后, 我们讨论对于密码学有重要价值的完全数、梅森素数和费马素数等概念.

学习本章之后，我们应该能够

- 掌握整除和带余除法的概念与性质，以及相关的计算方法及应用；
- 掌握最大公因子和辗转相除的概念与性质，以及相关的计算方法及应用；
- 了解连分数的概念与性质及其在 RSA 的 Wiener 攻击中的应用；
- 了解完全数、梅森素数和费马素数的概念及相关性质.

1.1 整除与带余除法

在数集的表示中，我们通常用$\mathbb{N}$表示正整数（自然数）集合, 即$\mathbb{N}=\{1,2,3,\ldots\}$；用$\mathbb{Z}$表示整数集合, 即$\mathbb{Z}=\{\ldots,-3,-2,-1,0,1,2,3,\ldots\}$. 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 1.1.1 设$a,b\in\mathbb{Z},b\neq 0$. 如果存在 $q\in\mathbb{Z}$使得 $a=qb$, 那么就称 a 可被 b **整除**或者称 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 1.1.2 若 b 为 a 的因子, 且 $b\neq 1, b\neq a$, 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, 但不是其真因子.

定理 1.1.1 设 $a, b\in\mathbb{Z}$, 则有

(1) $b|a\Leftrightarrow -b|a\Leftrightarrow b|-a\Leftrightarrow |b||a|$;

(2) 设 $a\neq 0$, 如果 $b|a$, 那么$|b|\leqslant|a|$.

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 $q\in\mathbb{Z}$.

(2) 由(1)知$|a|=|q||b|$. 当$a \neq 0$时, $|q| \geqslant 1$.

□

定理 1.1.2 设 $a, b, c \in \mathbb{Z}$,

(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 $m, n \in \mathbb{Z}$ 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$a = q_1 b,\ b = q_2 c$, 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$a = q_1 b,\ c = q_2 b$, 从而

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

必要性得证. 取 $m = 1, n = 0$ 及 $m = 0, n = 1$ 就可以推出充分性.

□

我们可以将 $ma+nc$ $(m, n \in \mathbb{Z})$〉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 1.1.1 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

$$a = q_1 b,\ b = q_2 a,$$

可得$a = q_1 q_2 a$. 由于$a \neq 0$, 所以$q_1 q_2 = 1,\ q_1 = q_2 = \pm 1$. 从而$b = \pm a$.

□

例 1.1.2 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 1.1.2(4), 则 $a|2tn-an$. 由 $a = 2t-1$ 知 $2tn-an = 2tn-2tn + n = n$. 代入即得 $a|n$.

□

例 1.1.3 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 1.1.2(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, 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 $b\in\mathbf{S}$, 都有 $a<b$ 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, 只能够作为公理给出, 它是我们证明下面一些定理的关键基础和依据.

定理 1.1.3 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

$$a = qb + r, \quad 0\leqslant r<b. \tag{1.1.1}$$

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

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

这个集合是非负整数的集合, 且不是空集: 因为 $b\geqslant 1$, 所以$|a|b\geqslant|a|$, 那么

$$a - (-|a|)b = a+|a|b\geqslant a+|a|\geqslant 0.$$

即当 $x=-|a|$时, $a-xb\in\mathbf{S}$. 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

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

我们也能够证明 $r<b$: 因为如果 $r<b$ 不成立, 则 $r\geqslant b$, 那么

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

所以 $a - (q+1)b\in\mathbf{S}$. 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(1.1.1)式, 即

$$a = q_1b + r_1, \quad 0\leqslant r_1<b. \tag{1.1.2}$$

设 $r<r_1$, 则 $0<r_1-r<b$. 将(1.1.1)和(1.1.2)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 1.1.1(2)）. 同理如果设 $r_1<r$, 也会导出矛盾. 所以 $r = r_1$, 进而 $q = q_1$. 唯一性得证.

□

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 $a = q_1(-b) + r$, $0\leqslant r<-b$. 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 $a = qb + r$, $0\leqslant r<|b|$.

显然, $b|a$ 的充要条件是 $r=0$. 注意 a 与$-a$（$a\neq 0$）余数不同，但两个余数之和为$|b|$. 例如, 如果用 7 去除 60 和−60, 得到 $60 = 7\times 8+4$ 和$-60=7\times(-9)+3$.

定义 1.1.3 设 $a, q, r\in\mathbb{Z}$, 满足 $a = 2q + r$, $0\leqslant r<2$. 若 $r = 0$, 称 a 为**偶数**；若 $r = 1$, 则称 a 为**奇数**.

定义 1.1.4 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 1.1.4 素数有无穷多个.

证明 用反证法. 假定只有有限个素数 $p_1, p_2, \ldots, p_k$, 考虑$a = p_1p_2 \cdot \cdots \cdot p_k + 1$. 由于 a 是合数, 所以它必有素因子, 不妨假定这个素因子为 $p_j(1 \le j \le k)$, 显然 $p_j|a$. 因为

$$a - p_1p_2 \cdot \cdots \cdot p_k = 1,$$

又$p_j|p_1p_2 \cdot \cdots \cdot p_k$, 故$p_j|1$. 但是素数$p_j \geqslant 2$, 所以$p_j|1$是不可能的. 因此推出矛盾, 假设错误.

□

定理 1.1.5 对任意正整数 n, 存在素数 p 满足 $n<p\leqslant n! + 1$.

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 满足 $p|a$. 先假定 $p\leqslant n$, 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.

□

注意，该定理也同时证明了素数有无穷多个.

定理 1.1.6 如果整数 $n\geqslant 2$, 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

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

定理得证.

□

定理 1.1.7 若 n 为合数, 则 n 必有素因子 p 满足$p \le \sqrt{n}$.

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 $p\leqslant r$ 且 $p\leqslant s$. 所以$p^2\leqslant rs = n$, 即$p \le \sqrt{n}$.

□

定理 1.1.7 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 $p \le \sqrt{a} \le \sqrt{x}$, 所以只要先求出$\sqrt{x}$以内的全部素数$\{p_i, 1 \le i \le k\}$（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 1.1.4 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 1.1

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. 证明整数$Q_n = n^3 + 1$ $(n>1)$是合数.
4. 证明任意三个连续的正整数的乘积都被 6 整除.
5. 证明每个奇数的平方都具有 $8k+1$ 的形式.

B 组

6. 证明若$m - p|mn + pq$, 则$m - p|mq + np$.
7. 证明若 a 是整数, 则 $a^3 - a$ 能被 3 整除.
8. 假设把所有的素数按从小到大排列，p_k 表示第 k 个素数，证明素数$p_n \leqslant p_1 p_2 \cdot \cdots \cdot p_{n-1} + 1$ 对于所有的 $n \geqslant 3$ 成立.
9. 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.
10. 编写程序求 1 000 000 内的所有素数.

1.2 最大公因子与辗转相除法

定义 1.2.1 设 $a_1, a_2, \ldots, a_n$ 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 $a_1, a_2, \ldots, a_n$ 的一个**公因子**. 在整数 $a_1, a_2, \ldots, a_n$ 的所有公因子中最大的一个称为**最大公因子**, 记作$(a_1, a_2, \ldots, a_n)$或者 $\gcd(a_1, a_2, \ldots, a_n)$. 特别地, 若$(a_1, a_2, \ldots, a_n) = 1$, 我们称 $a_1, a_2, \ldots, a_n$ **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$(a_1, a_2, \ldots, a_n)$本身就包含了条件 $a_1, a_2, \ldots, a_n$ 不全为零.

定理 1.2.1 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 $(a, b) \leqslant (b, c)$. 同理可证$(b, c) \leqslant (a, b)$, 于是$(a, b) = (b, c)$. 定理得证.

□

结合带余除法, 我们可以得到这样的结论, 即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**欧几里得算法**.

任给两个正整数 a 和 b, 不妨设 $a \geqslant b$, 由定理 1.1.3, 有下列等式:

$$\begin{aligned} a &= bq_1 + r_1, \quad 0 < r_1 < b, \\ b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1, \\ &\vdots \\ r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_{n+1} + r_{n+1}, \quad r_{n+1} = 0. \end{aligned} \tag{1.2.1}$$

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(1.2.1)式中$r_{n+1} = 0$.

定理 1.2.2 若任给两个正整数 a 和 b, 则(a, b)就是(1.2.1)式中最后一个不等于零的余数, 即$(a, b) = r_n$.

证明 由定理 1.2.1 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 1.2.2 实际上给出了计算两个正整数最大公因子的算法, 即著名的欧几里得算法, 请读者自行编程实现.

定理 1.2.3 对任意两个正整数 a 和 b, 一定存在两个整数 m 和 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(1.2.1)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(1.2.1)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 和 n, 使得 $r_n = ma + nb$. 又根据定理 1.2.2 知$(a,$

$b) = r_n$, 定理得证.

□

显然, 定理 1.2.3 中 a 和 b 的取值可推广到全部整数范围.

例 1.2.1 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

$$
\begin{aligned}
4 &= 16 - 12\times 1 && \text{初始步骤}\\
&= 16 - (44 - 16\times 2) && \text{回代步骤}\\
&= 16\times 3 - 44 && \text{整理步骤}\\
&= (104 - 44\times 2)\times 3 - 44 && \text{回代步骤}\\
&= 104\times 3 - 44\times 7 && \text{整理步骤}\\
&= 104\times 3 - (772 - 104\times 7)\times 7 && \text{回代步骤}\\
&= 104\times 52 - 772\times 7 && \text{整理步骤}\\
&= (876 - 772\times 1)\times 52 - 772\times 7 && \text{回代步骤}\\
&= 876\times 52 - 772\times 59 && \text{整理步骤}\\
&= 876\times 52 - (7\,780 - 876\times 8)\times 59 && \text{回代步骤}\\
&= 876\times 524 - 7\,780\times 59 && \text{整理步骤}\\
&= (8\,656 - 7\,780\times 1)\times 524 - 7\,780\times 59 && \text{回代步骤}\\
&= 8\,656\times 524 - 7\,780\times 583 && \text{整理步骤}\\
&= 8\,656\times 524 + (-7\,780)\times 583, && \text{规范步骤}
\end{aligned}
$$

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

证明 由定理 1.2.3 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 1.2.5 设有整数 a, b, c, 其中 $c>0$, 则$(ac, bc) = (a, b)c$.

证明 由定理 1.2.3 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 1.2.4 可知$(a, b)c|(ac, bc)$.

因此, $(ac, bc) = (a, b)c$.

□

例 1.2.2 设 $a = 16\times2\ 350$, $b = 27\times2\ 350$, 求(a, b).

解 $(a, b) = (16,27) \times2\ 350 = 1\times2\ 350 =2\ 350$.

□

例 1.2.3 证明：若整数 a, b, d 满足 $d|a$, $d|b$, 则

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

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

证明 因为 $d|a$, $d|b$, 则由定理 1.2.5 我们有

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

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

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

□

定理 1.2.6 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 1.2.3, 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 与 b 互素. 充分性得证.

□

定理 1.2.7 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 1.2.6 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 $a|c$.

□

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 1.2.8 设 $a_1, a_2, \ldots, a_n$ 是 n 个整数, 其中 $a_1\neq 0$. 令

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

则

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

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 $d_n|a_{n-1}$, $d_n|d_{n-2}$. 以此类推, 可得

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

故 d_n 是 $a_1, a_2, \ldots, a_n$ 的公因子.

不妨设 d 为 $a_1, a_2, \ldots, a_n$ 的任意公因子. 因为 $d|a_1$, $d|a_2$, 则由定理 1.2.4 我们有 $d|d_2$, 又 $d|a_3$, 则 $d|d_3$. 以此类推, 可得 $d|d_n$. 故 $d\leqslant d_n$.

根据最大公因子的定义, 可知

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

□

例 1.2.4 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 1.2.2 设 $a_1, a_2, \ldots, a_n$ 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 $a_1, a_2, \ldots, a_n$ 的所有公倍数中最小的正整数称为**最小公倍数**, 记作$[a_1, a_2, \ldots, a_n]$（或者 $\mathrm{lcm}(a_1, a_2, \ldots, a_n)$）.

例如, 12 和−18 的公倍数为$\{\pm 36, \pm 72, \ldots\}$, 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$[a_1, a_2, \ldots, a_n] = [|a_1|, |a_2|, \ldots, |a_n|]$. 于是, 我们先讨论两个正整数的最小公倍数的求法.

定理 1.2.9 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 $ab \leqslant m$. 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 1.2.10 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) $[a,b] = \dfrac{ab}{(a,b)}$.

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 1.2.9, 有$[a_1,b_1] = a_1b_1$, 即

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

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 1.2.11 设 $a_1, a_2, \ldots, a_n$ 是 n 个整数, 令

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

则

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

证明 因为 $m_i|m_{i+1}$ $(i = 2,3,\ldots,n-1)$, 且 $a_1|m_2$, $a_i|m_i$ $(i = 2,3,\ldots,n)$, 所以 m_n 是 $a_1,a_2,\ldots,a_n$ 的公倍数. 又设 m 是 $a_1, a_2, \ldots, a_n$ 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 $m_3|m$. 以此类推, 最后得 $m_n|m$, 因此 $m_n \leqslant |m|$. 所以 $m_n = [a_1, a_2, \ldots, a_n]$. 定理得证.

□

例 1.2.5 计算[90, 30, 114, 42, 81].

解 因为

$$[90, 30]=\frac{90\times30}{(90, 30)}=\frac{90\times30}{30}=90,$$

$$\left[90, 114\right]=\frac{90\times114}{(90, 114)}=\frac{90\times114}{6}=1\ 710,$$

$$[1\ 710, 42]=\frac{1\ 710\times42}{(1\ 710, 42)}=\frac{1\ 710\times42}{6}=11\ 970,$$

$$[11\ 970, 81]=\frac{11\ 970\times81}{(11\ 970, 81)}=\frac{11\ 970\times81}{9}=107\ 730,$$

所以[90, 30, 114, 42, 81] = 107 730.

□

定理 1.2.12 设 $a_1, a_2, \ldots, a_n$ 是 n 个正整数, 如果 $a_1|m, a_2|m, \ldots, a_n|m$, 则

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

证明 对 n 用数学归纳法.

当 $n = 2$ 时, 由定理 1.2.10 可知命题成立.

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

当 $n = k + 1$ 时, 由

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

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

□

习题 1.2

A 组

1. 求以下整数对的最大公因子：

   (1) (55, 85); (2) (−15, −35); (3) (−90, 100);

   (4) (202, 282); (5) (666, 1 414); (6) (20 785, 44 350).

2. 求以下整数的最大公因子：

   (1) (10, 22, 55); (2) (98, 105, 280); (3) (280, 330, 405, 490).

3. 设 a, b 取值如下，运用欧几里得算法, 求(a,b)和整数 m,n, 使 $ma + nb = (a,b)$.

   (1) (51, 87); (2) (102, 222); (3) (981, 1 234); (4) (34 709, 100 313).

4. 求以下整数对的最小公倍数：

   (1) (16, 60); (1) (28, 36); (3) (231, 732); (4) (−871, 728).

5. 证明若整数 a, b 满足$(a, b) = 1$, 则$(a+b, a−b) = 1$ 或 2.

6. 证明若整数 a, b 满足$(a, b) = 1$, 则$(a+b, a^2+b^2) = 1$ 或 2.

7. 证明若 k 为正整数, 则 $3k+2$ 与 $5k+3$ 互素.

8. 证明若 m, n 为正整数, a 是大于 1 的整数. 则有$(a^m −1, a^n −1) = a^{(m, n)} −1$.

9. 设 a, b 是正整数，证明若$[a, b]=(a, b)$, 则 $a = b$.

B 组

10. 求如下整数对的最大公因子：

(1) $(2n+1, 2n-1)$; (2) $(kn+1, k(n+2))$; (3) $(2n^2+6n-4, 2n^2+4n-3)$.

11. 证明 $\sqrt[3]{5}$ 为无理数.

12. 证明$(n+1, n^2-n+1)=1$ 或 3, $n\in\mathbb{Z}^+$.

13. 证明 $12|n^4+2n^3+11n^2+10n$, $n\in\mathbb{Z}$.

14. 设 $3|a^2+b^2$, 证明 $3|a$ 且 $3|b$.

15. 设 n, k 是正整数, 证明 n^k 与 n^{k+4} 的个位数字相同.

16. 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.

17. 设 a 是自然数, 问 a^4-3a^2+9 是素数还是合数？

18. 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.

19. 设 f_k 表示斐波那契数列的第 k 个数，证明$(f_m, f_n)=f_{(m, n)}$.

20. 编写程序计算整数 a, b 的最大公因子.

21. 编写程序计算整数 a, b 的最小公倍数.

1.3 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？接下来就讨论这个问题.

定理 1.3.1 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 和 n, 使得

$$ma+np=1,$$

所以

$$mab+npb=b.$$

由于 $p|ab$, 所以 $p|b$.

□

由定理 1.3.1，容易得到如下推论.

推论 1.3.1 设 p 为素数, 若$p|a_1a_2\cdot\cdots\cdot a_n$, 其中$a_1, a_2, \dots, a_n$是 n 个整数, 则$p|a_1$, $p|a_2$, …, $p|a_n$至少有一个成立.

证明 用数学归纳法.

当 $n=2$ 时, 根据定理 1.3.1, 显然成立.

假设 $n-1$ 时命题成立, 即若$p|a_1a_2\cdot\cdots\cdot a_{n-1}$, 则$p|a_1, p|a_2, \dots, p|a_{n-1}$至少有一个成立.

对于 n, 由于$p|(a_1a_2\cdot\cdots\cdot a_{n-1})a_n$, 所以$p|a_1a_2\cdot\cdots\cdot a_{n-1}$或$p|a_n$ 再根据归纳假设, 可知

$p|a_1, p|a_2, \ldots, p|a_{n-1}, p|a_n$至少有一个成立. 命题得证.

□

上面的定理 1.3.1 及推论 1.3.1 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|12 且 12 = 3×4, 但是 6∤3 且 6∤4.

定理 1.3.2 设 $a_1, a_2, \ldots, a_n, c$ 是整数, 如果$(a_i, c) = 1,\ 1 \le i \le n,$ 则$(a_1 a_2 \cdot \cdots \cdot a_n, c) = 1.$

证明 用反证法. 假设存在大于 1 的整数 m 满足$(a_1 a_2 \cdot \cdots \cdot a_n, c) = m,$ 则必存在素数 p, 使 $p|m$, 于是$p|a_1 a_2 \cdot \cdots \cdot a_n$且 $p|c$. 由推论 1.3.1, 可知 $p|a_1, p|a_2, \ldots, p|a_n$ 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 1.3.3 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

$$n = p_1 p_2 \cdot \cdots \cdot p_s, \quad p_1 \leqslant p_2 \leqslant \ldots \leqslant p_s, \tag{1.3.1}$$

其中 $p_1, p_2, \ldots, p_s$ 是素数, 并且若

$$n = q_1 q_2 \cdot \cdots \cdot q_l, \quad q_1 \leqslant q_2 \leqslant \ldots \leqslant q_t, \tag{1.3.2}$$

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

证明 首先, 用数学归纳法证明(1.3.1)式成立.

当 $n = 2$ 时, (1.3.1)式显然成立.

假设对于一切大于 1 且小于 n 的正整数, (1.3.1)式都成立.

对于正整数 n, 若 n 是素数, 则(1.3.1)式对 n 成立.

若 n 是合数, 则存在正整数 b,c 满足条件

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

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(1.3.1)式成立.

下面证明唯一性.

假设对 n 同时有(1.3.1)和(1.3.2)两式成立, 则

$$p_1 p_2 \cdot \cdots \cdot p_s = q_1 q_2 \cdot \cdots \cdot q_t. \tag{1.3.3}$$

由定理 1.3.1 可知, $\exists p_k, q_j$ 使得 $p_1|q_j, q_1|p_k,$ 但由于 p_k 和 q_j 均为素数, 故 $p_1 = q_j, q_1 = p_k.$ 又 $p_1 \leqslant p_k, q_1 \leqslant q_j,$ 故同时有 $p_1 \leqslant q_1, q_1 \leqslant p_1,$ 因此 $p_1 = q_1,$ 由(1.3.3)式得

$$p_2 p_3 \cdot \cdots \cdot p_s = q_2 q_3 \cdot \cdots \cdot q_t.$$

同理可得 $p_2 = q_2, p_3 = q_3,$ 以此类推, 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(1.3.2)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 1.3.2 任一大于 1 的整数都能够唯一地表示成

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \cdots \cdot p_s^{\alpha_s}, \quad \alpha_i > 0, \quad i = 1,2, \ldots, s, \tag{1.3.4}$$

其中 $p_i < p_j$ $(i < j)$ 是素数.

(1.3.4)式称为 n 的**标准分解式**.

定理 1.3.4 设 n 是大于 1 的任一整数, 其标准分解式由(1.3.4)式给出, 那么 d 是 n 的正因子的充要条件是

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdot \cdots \cdot p_s^{\beta_s},\ \alpha_i \geqslant \beta_i \geqslant 0,\quad i = 1,2,\ldots,s. \tag{1.3.5}$$

证明 先证充分性. 若(1.3.5)式成立, 则存在正整数

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

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

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

则必有

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

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

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

又由 $p_1^{\alpha_1} > 0$, 可得

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

根据定理 1.3.1 的推论 1.3.1, 可知存在 k 满足 $2 \leqslant k \leqslant s$, 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就都可以知道了, 且可以由(1.3.5)式给出. 我们不难得出以下定理.

定理 1.3.5 设正整数 n 的标准分解式为

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

$\tau(n)$ 表示 n 的所有正因子的个数, 则

$$\begin{aligned}\tau(n) &= \tau\left(p_1^{\alpha_1}\right) \cdot \tau\left(p_2^{\alpha_2}\right) \cdot \cdots \cdot \tau\left(p_s^{\alpha_s}\right) \\ &= (\alpha_1 + 1)(\alpha_2 + 1) \cdot \cdots \cdot (\alpha_n + 1),\quad \alpha_i > 0,\ i = 1,2,\ldots,s.\end{aligned}$$

该定理显然成立，感兴趣的读者可以自己证明.

例 1.3.1 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 1.3.6 设 a,b 为两个正整数, 其素因子分解式分别为

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

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

那么

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

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

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 0, 所以这个结果和定理 1.2.10 中已经证明过的结果相同.

□

例 1.3.2 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

$$90 = 2\times3^2\times5,$$

$$30 = 2\times3\times5,$$

$$114 = 2\times3\times19,$$

$$42 = 2\times3\times7,$$

$$81 = 3^4,$$

于是

$$(90,30) = 2\times3\times5 = 30,$$

$$(30,114) = 2\times3 = 6,$$

$$(6,42) = 2\times3 = 6,$$

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

所以整数 90,30,114,42,81 的最大公因子是 3.

由于

$$[90,30] = 2\times3^2\times5 = 90,$$

$$[90,114] = 2\times3^2\times5\times19 = 1\ 710,$$

$$[1\ 710,42] = 2\times3^2\times5\times7\times19 = 11\ 970,$$

$$[11\ 970,81] = 2\times3^4\times5\times7\times19 = 107\ 730,$$

所以整数 90,30,114,42,81 的最小公倍数是 107 730.

□

例 1.3.3 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

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

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

$$c = p_1^{\gamma_1} p_2^{\gamma_2} \cdot \cdots \cdot p_s^{\gamma_s},\ \gamma_i \geqslant 0,\ i = 1,2,\ldots,s,$$

则

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

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

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

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

不难验证，对于$i = 1,2,\ldots,s$，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 1.3.4 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

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

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

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

取

$$c = p_1^{\alpha_1} p_2^{\alpha_2} \cdot \cdots \cdot p_t^{\alpha_t}, \qquad d = p_{t+1}^{\beta_{t+1}} p_{t+2}^{\beta_{t+2}} \cdot \cdots \cdot p_s^{\beta_s}$$

即为所求.

□

习题 1.3

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) 2 154; (3) 2 838; (4) 3 288.

3. 求以下整数的所有正因子的个数：

   (1) 1 260; (2) $2\times3^2\times5\times7^2\times11^5\times13^5\times17^{19}\times19$.

4. 求以下整数的最大公因子与最小公倍数：

   (1) (15, 60, 168, 66, 286); (2) (30, 180, 210, 55, 125).

5. 设 p 是一个素数，a 是一个整数，n 是一个正整数，证明如果 $p|a^n$，则 $p|a$.

6. 设 a, b, c 是三个正整数，证明$[(a,b), (a,c), (b,c)] = ([a,b], [a,c], [b,c])$.

7. 设 rad(n)表示整数 n 的所有不同素因子的乘积，证明 rad(n) = n 的充要条件是 n 为无平方

因子数. 并说明等号在什么情况下成立.

B 组

8. 写出 22 345 680 的标准分解式.

9. 设 a, b, c 是三个正整数, 证明如果$(a, b) = 1$ 且 $ab = c^n$, 则存在正整数 d 和 e, 满足 $a = d^n$ 且 $b = e^n$.

10. 证明在 1, 2, 3, …, $2n$ 中任取 $n + 1$ 数, 其中至少有一个能被另一个整除.

11. 证明$1+\frac{1}{2}+\cdots+\frac{1}{n}$（$n \geqslant 2$）不是整数.

12. 设 a, b 是正整数. 证明存在 a_1, a_2, b_1, b_2, 使得 $a = a_1a_2, b = b_1b_2, (a_2, b_2) = 1$, 并且$[a, b] = a_2b_2$.

13. 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.

14. 设 p 是一个素数, n 是一个正整数. 如果 $p^a|n$, 但 $p^{a+1}\nmid n$, 我们称 p^a 正好整除 n, 记为 $p^a\|n$.

    (1) 证明如果 $p^a|m$ 且 $p^b|n$, 则 $p^{a+b}\|mn$.

    (2) 证明如果 $p^a|m$, 则 $p^{ka}\|m^k$.

    (3) 证明如果 $p^a|m, p^b|n$ 且 $a \neq b$, 则 $p^{\min(a, b)}\|(m+n)$.

15. 设 rad(n)表示整数 n 的所有不同素因子的乘积，对于正整数 a 和 b, 证明 rad(ab) $\leqslant$rad(a)rad(b), 并说明等号在什么情况下成立.

*1.4[Θ] 连分数

本节内容与 1.2 节的辗转相除法有密切关系, 我们可以利用辗转除法来求有理数的连分数表示形式. 另外，利用连分数可以巧妙地构造针对 RSA[1]公钥加密系统的攻击方案，RSA 是最早、至今最常用的公钥密码系统之一.

1.4.1 连分数的定义和性质

我们首先给出连分数的定义.

定义 1.4.1 设 $a_0, a_1, a_2, \ldots, a_n$ 是一个实数列, 除 a_0 以外都大于 0. 对于整数 $n \geqslant 0$, 我们将分数

[Θ] 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。

[1] RSA 是 1977 年由罗纳德·李维斯特（Ron Rivest）、阿迪·萨莫尔（Adi Shamir）和伦纳德·阿德曼（Leonard Adleman）一起提出的一种公钥密码算法体制。

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\ddots+\cfrac{1}{a_n}}}} \tag{1.4.1}$$

叫作 n 阶**有限连分数**. 当 a_0 是整数, a_1, a_2, …, a_n 都是正整数时, 分数(1.4.1)叫作 n 阶**有限简单连分数**. 为了书写方便, 我们将(1.4.1)式简记为

$$[a_0; a_1, \ldots, a_n]. \tag{1.4.2}$$

我们将有限连分数

$$[a_0; a_1, \ldots, a_k], 0\leqslant k\leqslant n \tag{1.4.3}$$

叫作有限连分数(1.4.1)式的第 k 个**渐进分数**.

当(1.4.1)式中的 $n\to\infty$ 时, 则分数

$$a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3+\ddots}}} \tag{1.4.4}$$

叫作**无限连分数**, 可简记为

$$[a_0; a_1, a_2, \ldots]. \tag{1.4.5}$$

当 a_0 是整数, a_1,…,a_n 都是正整数时, 分数(1.4.4)叫作**无限简单连分数**. 我们将有限连分数

$$[a_0; a_1, \ldots, a_k], k\geqslant 0 \tag{1.4.6}$$

叫作无限连分数(1.4.4)的第 k 个**渐进分数**.

对于无限连分数, 我们有时也将其表示为

$$[a_0; a_1, \ldots, a_n],$$

但这里 $n\to\infty$.

定理 1.4.1 若使连分数$[a_0; a_1, \ldots, a_n]$的渐进分数分别为

$$[a_0; a_1, \ldots, a_i] = \frac{p_i}{q_i}, \quad 0\leqslant i\leqslant n,$$

则这些渐进分数间有关系

$$p_0 = a_0, \quad p_1 = a_1a_0+1, \quad \ldots, \quad p_k = a_k p_{k-1}+p_{k-2},$$

$$q_0 = 1, \quad q_1 = a_1, \quad \ldots, \quad q_k = a_k q_{k-1}+q_{k-2},$$

其中 $2\leqslant k\leqslant n$.

证明 用数学归纳法.

因为

$$\frac{p_0}{q_0}=a_0,\ \frac{p_1}{q_1}=a_0+\frac{1}{a_1}=\frac{a_1a_0+1}{a_1},$$

$$\frac{p_2}{q_2}=a_0+\frac{1}{a_1+\dfrac{1}{a_2}}=\frac{a_2a_1a_0+a_2+a_0}{a_2a_1+1},$$

所以当 $k=0,1,2$ 时可直接验证.

假设当 $k=m$ $(2\leqslant m<n)$时, 命题成立, 即

$$[a_0;\ a_1,\ \ldots,\ a_m]=\frac{p_m}{q_m}=\frac{a_mp_{m-1}+p_{m-2}}{a_mq_{m-1}+q_{m-2}},$$

则当 $k=m+1$ 时, 有

$$\begin{aligned}[a_0;a_1,\cdots,a_m,a_{m+1}]&=[a_0;a_1,\cdots,a_m+\frac{1}{a_{m+1}}]\\&=\frac{(a_m+\dfrac{1}{a_{m+1}})p_{m-1}+p_{m-2}}{(a_m+\dfrac{1}{a_{m+1}})q_{m-1}+q_{m-2}}\\&=\frac{a_{m+1}(a_mp_{m-1}+p_{m-2})+p_{m-1}}{a_{m+1}(a_mq_{m-1}+q_{m-2})+q_{m-1}}\\&=\frac{a_{m+1}p_m+p_{m-1}}{a_{m+1}q_m+q_{m-1}}\\&=\frac{p_{m+1}}{q_{m+1}}\end{aligned}$$

定理得证.

□

定理 1.4.2 若连分数$[a_0;\ a_1,\ \ldots,\ a_n]$的渐进分数分别为

$$[a_0;\ a_1,\ \ldots,\ a_k]=\frac{p_k}{q_k},\quad 0\leqslant k\leqslant n,$$

则 p_k 和 q_k 满足

$$p_kq_{k-1}-p_{k-1}q_k=(-1)^{k-1},\quad 1\leqslant k\leqslant n, \tag{1.4.7}$$

$$p_kq_{k-2}-p_{k-2}q_k=(-1)^ka_k,\quad 2\leqslant k\leqslant n. \tag{1.4.8}$$

证明 用数学归纳法.

当 $k=1$ 时, (1.4.7)式显然成立.

假设当 $k=m-1$ $(1<m\leqslant n)$时, 命题成立, 即

$$p_{m-1}q_{m-2}-p_{m-2}q_{m-1}=(-1)^{m-2}=(-1)^m,$$

则当 $k=m$ 时, 由定理 1.4.1, 有

$$\begin{aligned} p_m q_{m-1} - p_{m-1} q_m &= (a_m p_{m-1} + p_{m-2}) q_{m-1} - p_{m-1}(a_m q_{m-1} + q_{m-2}) \\ &= -(p_{m-1} q_{m-2} - p_{m-2} q_{m-1}) \\ &= (-1)^{m-1} \end{aligned}$$

于是(1.4.7)式成立.

由(1.4.7)式和定理 1.4.1 可得

$$\begin{aligned} p_k q_{k-2} - p_{k-2} q_k &= (a_k p_{k-1} + p_{k-2}) q_{k-2} - p_{k-2}(a_k q_{k-1} + q_{k-2}) \\ &= a_k (p_{k-1} q_{k-2} - p_{k-2} q_{k-1}) \\ &= (-1)^k a_k \end{aligned}$$

于是(1.4.8)式成立.

□

定理 1.4.3 对于简单连分数, 我们有

(1) 当 $k \geqslant 2$ 时, $q_k \geqslant q_{k-1} + 1$, 因而对任何 k 来说, $q_k \geqslant k$;

(2) $\dfrac{p_{2k+1}}{q_{2k+1}} < \dfrac{p_{2k-1}}{q_{2k-1}}$, $\dfrac{p_{2k}}{q_{2k}} > \dfrac{p_{2k-2}}{q_{2k-2}}$, $\dfrac{p_{2k}}{q_{2k}} < \dfrac{p_{2k+1}}{q_{2k+1}}$;

(3) $\dfrac{p_k}{q_k}$ 为既约分数, 即 p_k 与 q_k 互素.

证明 (1) 根据定理 1.4.1, 显然有 $q_k \geqslant 1$, 又因为 $a_k \geqslant 1$, 所以当 $k \geqslant 2$ 时, 有

$$q_k = a_k q_{k-1} + q_{k-2} \geqslant q_{k-1} + 1.$$

又由 $q_0 = 1 > 0$, $q_1 = a_1 \geqslant 1$, 故用数学归纳法, 假设当 $k \geqslant 2$ 时,

$$q_{k-1} \geqslant k - 1,$$

则应用上面的结论可得

$$q_k \geqslant q_{k-1} + 1 \geqslant (k-1) + 1 = k.$$

于是(1)得证.

(2) 根据定理 1.4.2, 由

$$p_k q_{k-2} - p_{k-2} q_k = (-1)^k a_k,$$

即

$$\frac{p_k}{q_k} - \frac{p_{k-2}}{q_{k-2}} = \frac{(-1)^k a_k}{q_k q_{k-2}},$$

可知

$$\frac{p_{2k}}{q_{2k}}-\frac{p_{2k-2}}{q_{2k-2}}=\frac{(-1)^{2k}a_{2k}}{q_{2k}q_{2k-2}}=\frac{a_{2k}}{q_{2k}q_{2k-2}}>0,$$

即

$$\frac{p_{2k}}{q_{2k}}>\frac{p_{2k-2}}{q_{2k-2}}.$$

同理, 有

$$\frac{p_{2k+1}}{q_{2k+1}}-\frac{p_{2k-1}}{q_{2k-1}}=\frac{(-1)^{2k+1}a_{2k+1}}{q_{2k+1}q_{2k-1}}=\frac{-a_{2k}}{q_{2k}q_{2k-2}}<0,$$

即

$$\frac{p_{2k+1}}{q_{2k+1}}<\frac{p_{2k-1}}{q_{2k-1}}.$$

由

$$p_kq_{k-1}-p_{k-1}q_k=(-1)^{k-1},$$

即

$$\frac{p_k}{q_k}-\frac{p_{k-1}}{q_{k-1}}=\frac{(-1)^{k-1}}{q_kq_{k-1}},$$

可知

$$\frac{p_{2k+1}}{q_{2k+1}}-\frac{p_{2k}}{q_{2k}}=\frac{(-1)^{2k}}{q_{2k+1}q_{2k}}=\frac{1}{q_{2k+1}q_{2k}}>0,$$

即

$$\frac{p_{2k}}{q_{2k}}<\frac{p_{2k+1}}{q_{2k+1}}.$$

(3) 根据定理 1.4.2, 有

$$p_kq_{k-1}-p_{k-1}q_k=(-1)^{k-1}.$$

可知当 k 为奇数时, 存在整数 $x=q_{k-1}, y=-p_{k-1}$ 使

$$p_kx+q_ky=1,$$

当 k 为偶数时, 存在整数 $x=-q_{k-1}, y=p_{k-1}$ 使

$$p_kx+q_ky=1,$$

再根据定理 1.2.6, 可知 p_k 与 q_k 互素, 即 $\frac{p_k}{q_k}$ 为既约分数.

□

定理 1.4.4 每一个简单连分数表示一个实数.

证明 每一个有限简单连分数显然表示一个有理数. 我们考虑无限简单连分数

$$[a_0; a_1, \ldots, a_k, \ldots],$$

$\frac{p_k}{q_k}, k\geqslant 0$ 是它的渐进分数. 由定理 1.4.3 可知

$$\frac{p_0}{q_0}, \frac{p_2}{q_2}, \ldots, \frac{p_{2k}}{q_{2k}}, \ldots$$

是一个单调递增数列, 而

$$\frac{p_1}{q_1}, \frac{p_3}{q_3}, \ldots, \frac{p_{2k+1}}{q_{2k+1}}, \ldots$$

是一个单调递减数列, 且

$$\frac{p_1}{q_1} > \frac{p_{2k+1}}{q_{2k+1}} > \frac{p_{2k}}{q_{2k}} > \frac{p_0}{q_0},$$

所以这两个数列也是有界的. 又因为

$$0< \frac{p_{2k+1}}{q_{2k+1}} - \frac{p_{2k}}{q_{2k}} = \frac{1}{q_{2k+1}q_{2k}} \leqslant \frac{1}{2k(2k+1)},$$

而

$$\lim_{k\to\infty} \frac{1}{2k(2k+1)} = 0,$$

所以$\left[\frac{p_{2k}}{q_{2k}}, \frac{p_{2k+1}}{q_{2k+1}}\right](k = 0, 1, 2, \ldots)$作成一个区间套, 则 $\lim\limits_{k\to\infty} \frac{p_k}{q_k}$ 存在且唯一.

□

上面我们证明了任一简单连分数表示一个唯一的实数, 那么任一实数能否唯一地表示成简单连分数呢? 下面我们就来讨论这个问题.

首先, 我们给出一个直观的理解, 将一个有理数写成 $\frac{\text{分子}}{\text{分母}}$ 的形式, 当然我们也可以把它看作另一个的等效形式 $\frac{\text{被除数}}{\text{除数}}$, 由带余除法得到

$$\frac{\text{被除数}}{\text{除数}} = \text{商} + \frac{\text{余数}}{\text{除数}} = \text{商} + \frac{1}{\frac{\text{除数}}{\text{余数}}} = \text{商} + \frac{1}{\frac{\text{新的被除数}}{\text{新的除数}}} = \text{商} + \frac{1}{\text{新的商} + \frac{\text{新的余数}}{\text{新的除数}}},$$

那么,反复利用这个过程, 直到最新的余数为 0, 就会得到该有理数的连分数形式, 显然利用辗转相除法很快可以得到上式中的各个商. 上面过程的数学形式如下:

设 α 是一给定实数, 若 α 是有理数, 则 $\alpha = \frac{p}{q}$, 其中 p,q 为整数, 且 $q>0$. 由辗转相除法可得

$$\begin{aligned}
p &= a_0 q + r_1, && 0<r_1<q,\\
q &= a_1 r_1 + r_2, && 0<r_2<r_1,\\
&\vdots\\
r_{n-2} &= a_{n-1} r_{n-1} + r_n, && 0<r_n<r_{n-1},
\end{aligned}$$

$$r_{n-1} = a_n r_n + r_{n+1}, \qquad r_{n+1} = 0.$$

于是, 有理数 $\alpha = \dfrac{p}{q}$ 可以表示为如下的有限简单连分数：

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \ddots + \cfrac{1}{a_n}}}}$$

即 $\alpha = \dfrac{p}{q} = [a_0; a_1, \cdots, a_n]$. 因此, 任一有理数均可表示成有限简单连分数.

若 α 是无理数, 则由 $\alpha = [\alpha] + \{\alpha\}$, $0 < \{\alpha\} < 1$ 可得

$$\begin{aligned}
&\alpha = a_0 + \frac{1}{\alpha_1}, \qquad a_0 = [\alpha],\ \alpha_1 = \frac{1}{\{\alpha\}} > 1,\\
&\alpha_1 = a_1 + \frac{1}{\alpha_2}, a_1 = [\alpha_1], \qquad \alpha_2 = \frac{1}{\{\alpha_1\}} > 1,\\
&\qquad\qquad \vdots\\
&\alpha_k = a_k + \frac{1}{\alpha_{k+1}}, \quad a_k = [\alpha_k], \qquad \alpha_{k+1} = \frac{1}{\{\alpha_k\}} > 1,\\
&\qquad\qquad \vdots
\end{aligned}$$

于是, 我们有 $\alpha = [a_0; a_1, \cdots, a_k, \alpha_{k+1}]$, 显然 $\alpha_{k+1} = [a_{k+1}; a_{k+2}, \cdots\ ]$.

定理 1.4.5 任一无理数可表示成无限简单连分数.

证明 对于无理数 α, 通过上述步骤, 可知当 $k \geqslant 1$ 时, $a_k = [\alpha_k] \geqslant 1$, 于是我们只要证明

$$\lim_{k\to\infty} [a_0; a_1, \cdots, a_k] = \alpha,$$

即

$$\lim_{k\to\infty} \frac{p_k}{q_k} = \alpha.$$

由于

$$\frac{p_k}{q_k} = \frac{a_k p_{k-1} + p_{k-2}}{a_k q_{k-1} + q_{k-2}},$$

故

$$\alpha=[a_0;a_1,\cdots,a_k+\frac{1}{\alpha_{k+1}}]$$
$$=\frac{(a_k+\frac{1}{\alpha_{k+1}})p_{k-1}+p_{k-2}}{(a_k+\frac{1}{\alpha_{k+1}})q_{k-1}+q_{k-2}}$$
$$=\frac{\alpha_{k+1}(a_kp_{k-1}+p_{k-2})+p_{k-1}}{\alpha_{k+1}(a_kq_{k-1}+q_{k-2})+q_{k-1}}$$
$$=\frac{\alpha_{k+1}p_k+p_{k-1}}{\alpha_{k+1}q_k+q_{k-1}}$$

因此, 再根据定理 1.4.2, 我们有

$$\alpha-\frac{p_k}{q_k}=\frac{q_kp_{k-1}-q_{k-1}p_k}{q_k(\alpha_{k+1}q_k+q_{k-1})}=\frac{(-1)^k}{q_k(\alpha_{k+1}q_k+q_{k-1})}.$$

因为$\alpha_k>a_k$, 所以$\alpha_{k+1}q_k+q_{k-1}>q_{k+1}$, 又由定理 1.4.3, 可知

$$\left|\alpha-\frac{p_k}{q_k}\right|<\frac{1}{q_kq_{k+1}}\leqslant\frac{1}{k(k+1)}.$$

于是, 由$\lim\limits_{k\to\infty}\frac{1}{k(k+1)}=0$, 可知$\lim\limits_{k\to\infty}\frac{p_k}{q_k}=\alpha$.

□

我们已经知道了任一无理数可表示成无限简单连分数, 下面我们来证明其表示的唯一性.

定理 1.4.6 任一无理数只可表示成唯一的无限简单连分数.

证明 我们只需证明如果两个无限简单连分数

$$\alpha_0=[a_0;a_1,\cdots,a_k,\cdots],\qquad \beta_0=[b_0;b_1,\cdots,b_k,\cdots]$$

相等, 则 $a_k=b_k, k=0,1,2,\ldots$.

令$\alpha_k=[a_k;a_{k+1},\cdots]$, $\beta_k=[b_k;b_{k+1},\cdots]$, 则有

$$\alpha_k=a_k+\frac{1}{\alpha_{k+1}},\ \alpha_{k+1}>1,$$
$$\beta_k=b_k+\frac{1}{\beta_{k+1}},\ \beta_{k+1}>1,$$

于是

$$a_k=[\alpha_k],\qquad b_k=[\beta_k].$$

利用数学归纳法. 因为$\alpha_0=\beta_0$, 所以$a_0=[\alpha_0]=[\beta_0]=b_0$, 且有$\alpha_1=\beta_1$.

假设对于 k, 有$a_i=b_i$, $\alpha_{i+1}=\beta_{i+1}$, 其中 $i=1,2,\ldots,k$, 则对于 $k+1$, 我们有

$$a_{k+1}=[\alpha_{k+1}]=[\beta_{k+1}]=b_{k+1},$$

且 $\alpha_{k+2}=\beta_{k+2}$. 定理得证.

□

而有理数的情况有些特殊. 我们知道任一有限简单连分数表示一个有理数, 任一有理数均可表示成有限简单连分数, 但这种表示不是唯一的. 类似于无理数表示成无限简单连分数的唯一性的证明, 我们可得出以下结论.

定理 1.4.7 (1) 若有理分数 $\alpha=[a_0;a_1,\cdots,a_n]=[b_0;b_1,\cdots,b_m]$, 且 $a_n>1$, $b_m>1$, 则有

$$m=n,\quad a_i=b_i\ (i=0,1,\ldots,n).$$

(2) 任一有理分数 α 有且仅有两种有限简单连分数表示式, 即

$$\alpha=[a_0;a_1,\cdots,a_n]=[a_0;a_1,\cdots,a_n-1,1],$$

其中 $a_n>1$.

例 1.4.1 将 $\frac{547}{263}$ 表示成简单连分数.

解 由辗转相除法可得

$$547=2\times263+21$$
$$263=12\times21+11$$
$$21=1\times11+10$$
$$11=1\times10+1$$
$$10=10\times1$$

于是 $\frac{547}{263}=[2;12,1,1,10]=[2;12,1,1,9,1]$.

□

例 1.4.2 将 $\sqrt{3}$ 表示成简单连分数.

解 对于无理数 $\alpha=\sqrt{3}$, 我们有

$$a_0=[\sqrt{3}]=1,\ \alpha_1=\frac{1}{\sqrt{3}-1}=\frac{\sqrt{3}+1}{2},$$

$$a_1=[\alpha_1]=1,\ \ \alpha_2=\frac{2}{\sqrt{3}-1}=\sqrt{3}+1,$$

$$a_2=[\alpha_2]=2,\ \alpha_3=\frac{1}{\sqrt{3}-1}=\alpha_1,$$

于是 $\sqrt{3}=[1;1,2,1,2,\ldots]$.

□

定义 1.4.2 对于无限简单连分数$[a_0; a_1, a_2, \dots]$, 如果存在整数 $m \geqslant 0$, 且对于 m 存在正整数 k 使得对于所有 $n \geqslant m$, 有

$$a_{n+k} = a_k,$$

那么, 我们把这个无限简单连分数叫作**循环简单连分数**, 简称**循环连分数**, 记为

$$[a_0; a_1, \cdots, a_{m-1}, \overline{a_m, \cdots, a_{m+k-1}}].$$

显然, $\sqrt{3} = [1; \overline{1, 2}]$是循环连分数.

下面我们以定理的形式介绍一些关于利用连分数进行实数的有理逼近的结论, 但并不给出证明, 感兴趣的读者可以查阅相关书籍.

定理 1.4.8 令α是任意实数, $\frac{p_k}{q_k}$为α的第k个渐进分数. 那么, 对于任意的$0 < q \leq q_k$有

$$|\alpha - \frac{p_k}{q_k}| \leq |\alpha - \frac{p}{q}|.$$

因此, 在分母不超过q_k的所有分数中, $\frac{p}{q}$是α的最佳有理逼近.

定理 1.4.9 令α是任意实数, 那么α的连续两个渐进分数中的至少一个渐进分数满足

$$|\alpha - \frac{p}{q}| < \frac{1}{2q^2}.$$

定理 1.4.10 令α是任意实数. 若有理数$\frac{p}{q}$满足

$$|\alpha - \frac{p}{q}| < \frac{1}{2q^2},$$

那么$\frac{p}{q}$一定是α的一个渐进分数.

1.4.2 连分数的一个应用——RSA 的 Wiener 攻击

连分数的一项重要应用是对 RSA 公钥加密算法进行分析. 在本小节中, 我们将利用上一小节介绍的基础知识来设计一种小私钥情形下的对 RSA 算法的攻击手段. 首先简要介绍一下 RSA 公钥加密体制.

RSA 公钥加密算法是 Rivest, Shamir 和 Aldeman 于 1977 年提出的一种公钥加密体制, 是当前最常用的公钥加密算法之一. RSA 算法包括密钥生成, 加密和解密三个过程. 密钥生成过程包括如下步骤: 随机生成两个大素数p和q (通常来说, 选取的p和q的比特长度相同); 计算$N = p \cdot q$, 称作 RSA 的模数, 计算N的欧拉函数$\varphi(N) = (p-1)(q-1)$; 随机选取一个整数e, 其满足$1 < e < \varphi(N)$且$\big(e, \varphi(N)\big) = 1$; 利用扩展欧几里得算法计算得到一个整数$d$, 使其满足$de \equiv 1 (\mathrm{mod}\ \varphi(N))$. 令$(N, e)$为公钥, (p, q, d)为私钥. 加解密过程如下: 如果用户 B 想要将消息m的密文发送给用户 A, 那么 B 将使用 A 的公钥来计算得到密文$C =$

$m^e(\mathrm{mod}\ N)$然后将密文C发送给 A. A 接受到密文C后，使用私钥d来计算出明文$m = C^d(\mathrm{mod}\ N)$.

RSA 在使用过程中，为了加速 RSA 中的公钥加密（或验证）操作，人们会使用一个较小的加密指数 *e*. 另有一些时候，在某些应用场景中（例如智能卡），快速私钥解密（或签名）操作更为重要, 人们可能会倾向于选择一个较小的解密指数 *d*. 显然，这时将导致加密指数 *e* 的值很大，而且我们又不能为解密指数 *d* 选择太小的值，否则攻击者可以使用穷举搜索找到 *d*. Wiener 首次提出了小解密指数情形下的针对 RSA 算法的攻击手段, 并证明了若$d < \frac{1}{3} \cdot N^{1/4}$, 则攻击者可以快速地分解模数$N$.

Wiener 的连分数攻击过程如下：假设 RSA 模数 $N = p \cdot q$ 且 $q < p < 2q$; 此外, 假设攻击者知道解密指数$d < \frac{1}{3} \cdot N^{1/4}$, 且加密指数 *e* 提供给了攻击者. 此时 *d* 和 *e* 满足

$$e \cdot d = 1\ (\mathrm{mod}\ \varphi(\mathrm{N}))$$

其中$\varphi(N) = (p-1)(q-1)$.

我们注意到，上式意味着存在一个整数 *k* 使得

$$e \cdot d - k \cdot \varphi(\mathrm{N}) = 1.$$

因此，我们有

$$\left|\frac{e}{\varphi(\mathrm{N})} - \frac{k}{d}\right| = \frac{1}{d \cdot \varphi(\mathrm{N})}$$

由于 $N = p \cdot q$ 且 $q < p < 2q$，有

$$N - \varphi(N) = p + q - 1 < p + q < 3q < 3\sqrt{pq} = 3\sqrt{N}.$$

由此，我们可以认为分数$\frac{e}{N}$是分数$\frac{k}{d}$的近似值. 而且

$$\begin{aligned}\left|\frac{e}{N} - \frac{k}{d}\right| &= \left|\frac{ed - kN}{dN}\right| = \left|\frac{ed - k\varphi(N) - kN + k\varphi(N)}{dN}\right| \\ &= \left|\frac{1 - k(N - \varphi(N))}{dN}\right| \\ &\leq \frac{3k\sqrt{N}}{dN} = \frac{3k}{d\sqrt{N}}.\end{aligned}$$

由于$e < \varphi(\mathrm{N})$，显然我们有 $k < d$. 又由假设私钥$d < \frac{1}{3} \cdot N^{1/4}$，可得

$$\left|\frac{e}{N} - \frac{k}{d}\right| < \frac{1}{3d^2} < \frac{1}{2d^2}.$$

因此根据定理 1.4.10，我们可知分数$\frac{k}{d}$一定是有理数$\frac{e}{N}$的一个渐进分数.

因此, 当$d < \frac{1}{3} \cdot N^{1/4}$时, 我们可以得到一个高效的分解 RSA 模数$N$的算法: 首先计算$\frac{e}{N}$的每个渐进分数$\frac{k_i}{d_i}$, 然后计算$T_i = N - \frac{ed_i - 1}{k_i} + 1$; 对二次方程$y^2 - T_i y + N = 0$进行求解, 若解为$p$, 则$N$被分解; 若不是, 则继续计算$\frac{k_{i+1}}{d_{i+1}}$, 直到$N$被分解. 此时，我们不但对 *N* 进行了分

解，也得到了解密指数 d.

举例. 假设 RSA 模数 N=9 449 868 410 449，加密指数为 e=6 792 605 526 025，且被告知解密指数满足

$$d < \frac{1}{3} \cdot N^{1/4} \approx 584.$$

应用 Wiener 攻击，我们需要计算数

$$\alpha = \frac{e}{N}$$

的连分数展开，并检查每一个渐进分数的分母是否为解密指数 d. α 的连分数展开的渐进分数如下：

$$1，\frac{2}{3}，\frac{3}{4}，\frac{5}{7}，\frac{18}{25}，\frac{23}{32}，\frac{409}{569}，\frac{1\,659}{2\,308}，\cdots$$

依次检查每个分母，我们看到解密指数是由

$$d = 569$$

给出，它是第 7 个渐进分数的分母.

□

习题 1.4

A 组

1. 求以下有理数对应的简单连分数：

(1) $\frac{18}{13}$; (2) $\frac{19}{9}$; (3) $-\frac{931}{1005}$; (4) $\frac{831}{8110}$.

2. 求以下简单连分数对应的有理数：

(1) [2; 7]; (2) [1; 2, 3]; (3) [0; 5, 6]; (4) [3; 7, 15,1].

3. 求以下实数对应的简单连分数：

(1) $\sqrt{2}$; (2) $\sqrt{6}$; (3) $\sqrt{7}$; (4) $\frac{\sqrt{5}-1}{2}$.

4. 求以下无理数的无限简单连分数，前 6 个渐近分数，前 7 个完全商，以及该无理数和它的前 6 个渐近分数的差：

(1) $\sqrt{29}$; (2) $\frac{\sqrt{10}+1}{3}$.

B 组

5. 求以下实数对应的简单连分数：

(1) $\sqrt{59}$; (2) $\sqrt{29}$; (3) $1+\sqrt{259}$; (4) $\frac{2+\sqrt{5}}{3}$.

6. 设 a, b 是两个正整数，且 $b = ac$，证明$[b; a, b, a, b, a, \ldots] = \frac{b+\sqrt{b^2+4c}}{2}$.

7. 使用连分数算法编写程序，实现对输入正整数的因子分解，并使用所编写的程序验证整数 13 290 059 的两个素因子是否为 3 119 和 4 261.

*1.5 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, 尤其是关于具有一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 1.5.1 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 1.5.1 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 1.5.1 若正整数 n 的标准分解式为

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

则

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

证明 由定理 1.3.4 可知, n 的所有因子可表示为

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

故

$$\begin{aligned}\sigma(n)&=\sum_{x_1=0}^{\alpha_1}\sum_{x_2=0}^{\alpha_2}\cdots\sum_{x_s=0}^{\alpha_s}p_1^{x_1}p_2^{x_2}\cdot\cdots\cdot p_s^{x_s}\\&=\sum_{x_1=0}^{\alpha_1}p_1^{x_1}\cdot\sum_{x_2=0}^{\alpha_2}p_2^{x_2}\cdot\cdots\cdot\sum_{x_s=0}^{\alpha_s}p_s^{x_s}\\&=\frac{p_1^{\alpha_1+1}-1}{p_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{p_2-1}\cdot\cdots\cdot\frac{p_s^{\alpha_s+1}-1}{p_s-1}\end{aligned}$$

定理得证.

□

定理 1.5.2 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

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

所以 $2^{n-1}(2^n-1)$为完全数. 又显然有 $n\geqslant 2$, 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 $n\geqslant 2$, q 为奇数, 则有

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

故

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

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 $a=2^{n-1}(2^n-1)$. 定理得证.

□

于是,寻找偶完全数的问题就化为寻找形如 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 $2^{11}-1=2\,047=23\times 89$. 由此可见, 若 n 是素数, 2^n-1 不一定是素数.

定理 1.5.3 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 1.5.2 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 1.5.4　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 不是素数, 与已知条件矛盾. 所以 m 没有奇因子, 定理得证.

□

定义 1.5.3　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**.

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 $F_5=641\times6\,700\,417$, 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 1.5.5　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 $a>b\geqslant0$, $a=b+c$, $c>0$, 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.

□

习题 1.5

A 组

1. 判断以下整数是否为完全数：

(1) 36;　(2) 128;　(3) 496;　(4) 8 128.

2. 写出完全数判定算法.

3. 写出梅森素数判定算法.

4. 写出费马素数判定算法.

B 组

5. 编写程序寻找 10 000 以内的完全数.

6. 编写程序寻找 64 比特内的所有梅森素数.

7. 编写程序寻找 10 000 以内的费马素数.