第 1 章　整数的可除性

整数的可除性是数学中一个既基础又深邃的领域，它不仅是初等数学的核心概念之一，也是数论、近世（抽象）代数等数学分支的基石。从简单的整除、因数和倍数的概念出发，我们将逐步深入到素数与合数的判别、厄拉托塞师筛法的应用，以及欧几里德除法等工具的使用，这些构成了理解整数性质与结构的关键步骤。

本章将引领读者穿越整数的奇妙世界，探索整数之间的内在联系与规律。我们将看到，整数的可除性不仅关乎简单的除法运算，更蕴含着丰富的数学结构和深刻的数学原理。通过算术基本定理的阐述，我们将揭示整数分解的唯一性，理解素数在整数世界中的独特地位。同时，素数定理的引入，将为我们展示素数在自然数中分布的奥秘，让我们对整数的无限性与复杂性有更深刻的认识。

此外，本章还将介绍整数的进制表示、最大公因数与最小公倍数的计算、以及广义欧几里德除法等实用工具，这些工具不仅在数学理论中占据重要地位，也在信息安全、密码学、计算机科学等多个领域有着广泛的应用。

总之，整数的可除性是一个充满魅力的数学领域，它既是数学研究的基础，也是连接不同数学分支的桥梁。通过本章的学习，读者将能够更深入地理解整数的本质，掌握处理整数问题的基本方法，为后续的数学学习和研究打下坚实的基础。

本章的知识要点：

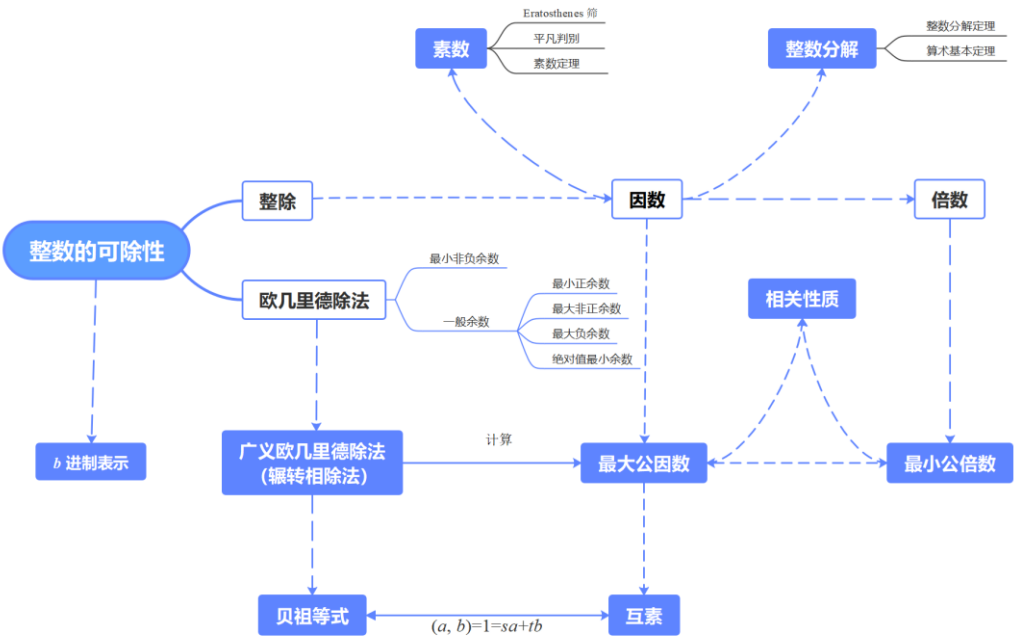

图 1-1　整数的可除性知识点图谱

1.1 整除 欧几里德除法 整数表示

1.1.1 整除的概念

在这节里，我们考虑关于整数的一些基本概念和性质：整除、素数、素数基本定理。

定义 1.1.1 设 a,b 是任意两个整数，其中 $b\neq 0$．如果存在一个整数 q 使得等式

$$a=bq \tag{1.1.1}$$

成立，就称 b **整除** a，或者 a 被 b 整除，记作 $b\mid a$，并把 b 叫做 a 的**因数**，把 a 叫做 b 的**倍数**.

否则，就称 b **不能整除** a 或者 a 不能被 b 整除，记作 $a\nmid b$.

此外，由于整数的乘法运算具有可以交换的性质，因此，q 也叫 a 的因数，我们常常将 q 写成 a/b 或 $\frac{a}{b}$.

注 1：：

0 是任何非零整数的倍数.

1 是任何整数的因数.

任何非零整数 a 是其自身的倍数，也是其自身的因数.

例 1.1.1： 3|21, -3|21, 3 ∤ 22, 5|0, 7|7.

注 2： 设 b_1，b_2，…，b_k 是它的所有因数，那么 $-b_1$，$-b_2$，…，$-b_k$ 也是它的所有因数，同时 $\frac{a}{b_1}$，$\frac{a}{b_2}$，…，$\frac{a}{b_k}$ 也是它的所有因数。

也就是说，

（1） 当 b 遍历整数 a 的所有因数时， $-b$ 也遍历整数 a 的所有因数.

（2） 当 b 遍历整数 a 的所有因数时， a/b 也遍历整数 a 的所有因数.

例 1.1. 2 105 = 3·35 = 5·21 = 7·15.

我们有 3, 5, 7 分别整除 105，或者 105 被 3, 5, 7 分别整除，

记作 3|105, 5|105, 7|105.

这时，3, 5, 7 都是 105 的因数，105 是 3, 5, 7 的倍数.

105 的所有因数是 $\{\pm 1,\pm 3,\pm 5,\pm 7,\pm 15,\pm 21,\pm 35,\pm 105\}$，

或是 $\{\mp 1,\mp 3,\mp 5,\mp 7,\mp 15,\mp 21,\mp 35,\mp 105\}$，

或是 $\{\pm 105=\frac{105}{\pm 1},\pm 35=\frac{105}{\pm 3},\pm 21=\frac{105}{\pm 5},\pm 15=\frac{105}{\pm 7},\pm 7=\frac{105}{\pm 15},\pm 5=\frac{105}{\pm 21},\pm 3=\frac{105}{\pm 35},\pm 1=\frac{105}{\pm 105}\}$.

下面，给出几个整除相关的结论：

定理 1.1.1 设 $a,b\neq 0,\ c\neq 0$ 是三个整数. 若 $c\mid b,\ b\mid a,$ 则 $c\mid a$.

证 设$c|b,\ b|a,$根据整除的定义，分别存在整数$q_1,\ q_2$使得

$$b=cq_1,\ a=bq_2$$

因此，我们有$a=bq_2=(cq_1)q_2=cq$.

因为$q=q_1q_2$是整数，所以根据整除的定义，有$c|a$.

例 1.1.3 因为 3|12, 12|36, 所以 3|36.

定理 1.1.2 设$a,b,c\neq 0$是三个整数. 若$c|a,\ c|b,$则$c|a\pm b$.

证 设$c|a,\ c|b,$那么存在两个整数$q_1,\ q_2$分别使得

$$a=cq_1,\ b=cq_2$$

因此，$a\pm b=cq_1\pm cq_2=c(q_1\pm q_2)$.

因为$q_1\pm q_2$是整数，所以$a\pm b$被c整除.

例 1.1.4 因为 5|25, 5|45, 所以 5|(25+45)=70, 5|(25-45)=-20.

定理 1.1.3 设$a,b,c\neq 0$是三个整数. 若$c|a,\ c|b,$则对任意整数$s,t,$有$c|sa+tb$.

证 设$c|a,\ c|b,$那么存在两个整数$q_1,\ q_2$分别使得

$$a=cq_1,\ b=cq_2$$

因此，$sa+tb=s(cq_1)+t(cq_2)=c(sq_1\pm tq_2)$

因为sq_1+tq_2是整数，所以$sa+tb$被c整除.

例 1.1.5 因为 3|6, 3|15, 所以 3|(2·6+5·15)=87, 3|(2·6-5·15)=-63.

推论 1.1.1：设$a,b,c\neq 0$是三个整数，$c|a,\ c|b.$如果存在整数$s,t,$使得$sa+tb=1$，则$c=\pm 1$.

证 设$c|a,\ c|b,$因为存在整数$s,t,$使得$sa+tb=1,$根据定理 1.1.3，我们有

$$c|sa+tb=1.$$

因此，$c=\pm 1$.

定理 **1.1.**3 可推广为多个整数的线性组合:

推论 1.1.2： 若整数$a_1,...,a_n$都是整数$c\neq 0$的倍数，则对任意n个整数$s_1,...,s_n,$整数$s_1a_1+...+s_na_n$是c的倍数.

例 1.1.6 因为 3|6, 3|15, 3|21, 所以 3|(2·6+5·15-2·21)=45.

定理 1.1.4 设 a,b 都是非零整数. 若 $a\mid b,\ \ b\mid a,$ 则 $a=\pm b$.

证 设 $a\mid b,\ \ b\mid a,$ 那么存在两个整数 $q_1,\ \ q_2$ 分别使得

$$a=bq_1,\quad b=aq_2.$$

从而，$a=bq_1=(aq_2)q_1=a(q_1q_2)$.

这样 $q_1q_2=1$，因为 q_1,q_2 是整数，所以 $q_1=q_2=\pm1$，进而，$a=\pm b$.

1.1.2 素数及其平凡判别

前面我们考虑了整除和因数，现在考虑不为 ±1 的不能继续分解的整数.

定义 1.1.2 设整数 $n\neq0,\ \ \pm1$. 如果除了显然的因数 ±1 和 $\pm n$ 外，n 没有其他因数，那么，n 叫做**素数**（或**质数**或**不可约数**），否则，n 叫做**合数**.

当整数 $n\neq0,\ \ \pm1$ 时，n 和 $-n$ 同为素数或合数. 因此，若没有特别声明，素数总是指正整数，通常写成 p.

例 1.1.7 整数 $2,\ 3,\ 5,\ 7$, 11 都是素数；而整数 4, 6, 8, 9, 10, 12, 14, 15 都是合数.

下面，我们给出关于素数的几个结论。首先给出的结论是每个合数必有素因子.

定理 1.1.5 设 n 是一个正合数，p 是 n 的一个大于 1 的最小正因数，则 p 一定是素数，且 $p\le\sqrt{n}$.

证 反证法. 如果 p 不是素数，则存在整数 q，$1<q<p,$ 使得 $q\mid p$.

但 $p\mid n,$ 根据定理 1.1.1，我们有 $q\mid n.$ 这与 p 是 n 的最小正因数矛盾. 所以，p 是素数.

因为 n 是合数，所以存在整数 n_1 使得 $n=pn_1,\quad 1<p\le n_1<n$.

因此，$p^2\le n,$（因为：p 是 n 的最小正因数），故 $p\le\sqrt{n}$.

定理 1.1.6 素数有无穷多个.

证 反证法. 假设只有有限个素数. 设它们为 $p_1,p_2,...,p_k,$ 考虑整数 $n=p_1\cdot p_2\cdots p_k+1$

因为 $n>p_i,\ i=1,...,k,$ 所以 n 一定是合数 (因为素数有限，n 又不是有限个素数中的一个).

根据定理 **1.1.5**，n 的大于 1 的最小正因数 p 是素数.

因此， p 是 $p_1, p_2, ..., p_k$ 中的一个，即存在 $j,\ 1 \le j \le k,$ 使得 $p = p_j$.

根据定理 **1.1.**2，我们有 $p \mid n - p_1 \cdots p_j \cdots p_k = 1$ 这是不可能的.

故，存在有无穷多个素数.

为了更好地描述数学概念和问题，我们引入数学符号.

数学符号 $\pi(x)$：设符号 $\pi(x)$ 表示不超过 x 的素数个数，即

$$\pi(x) = \sum_{p \le x} 1$$

是素数集的函数.

根据定理 1.1.6，存在无穷多个素数，这就是说， $\pi(x)$ 随 x 趋于无穷. 但人们希望知道 $\pi(x)$ 的具体公式. 为此，我们先给出一个基础性结论.

定理 1.1.7 （契贝谢夫不等式）设 $x \ge 2$. 则我们有

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

和

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

其中 p_n 中是第 n 个素数.

在此基础上，我们可以得到下面的结论.

定理 1.1.8（素数定理）

$$\lim_{x\to\infty} \pi(x)\frac{\ln x}{x} = 1.$$

在了解素数个数的相关结论之后，根据定理 1.1.5, 我们还可以得到一个整数为素数的平凡判别法则.

定理 1.1.9 (素数的平凡判别) 设 n 是一个正整数. 如果对所有的素数 $p \le \sqrt{n}$ ，都有 $p \nmid n$ ，则 n 一定是素数.

例 1.1.8 证明 89 是素数.

证：方法是先求出所有的 p，使得 $p \le \sqrt{89}$，并检验 $p \nmid 89$.

1）所有小于 $\sqrt{89}$ 的素数 p 为 $2,3,5,7$.

2）$p \nmid 89$.，因为 $p = 2,3,5,7$ 的倍数都不是 89.

所以，89 是素数.

1.1.3 Eratosthenes 筛法

为了更好地描述数学概念和问题，我们引入数学符号.

数学符号 [*x*] ： 设 x 是一个实数，$[x]$ 表示实数 x 的整数部分是小于或等于 x 的最大整数.

这时，我们有

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

例 1.1.9　[9.15]=9, [-9.15]=-10, [9]=9, [-9]=-9.

根据定理 **1.1.**9, 我们有一个寻找素数的确定性方法, 通常叫做**厄拉托塞师（Eratosthenes）筛法**（我们简称 E-筛法）.

定理 1.1.10 (E-筛法): 对任意给定的正整数 N ，求出所有不超过 N 的素数. 方法为: 列出 N 个整数，从中删除小于等于 $\sqrt{N}$ 的所有素数 $p_1,...,p_k$ 的倍数.

$$p_1 \text{ 的倍数: } \ 2p_1,...,\left[\frac{N}{p_1}\right]p_1;$$

$$\cdots \quad \cdots$$

$$p_k \text{ 的倍数: } \ 2p_k,...,\left[\frac{N}{p_k}\right]p_k;$$

余下的整数（不包括 1）就是所要求的不超过 N 的素数.

例 1.1.10 求出所有不超过 $N=100$ 的素数.

解 因为小于等于 $\sqrt{100}=10$ 的所有素数为 $2,3,5,7,$ 所以依次删除 $2,3,5,7,$ 的倍数,

2·2, 3·2, 4·2, …, 49·2, 50·2,
2·3, 3·3, 4·3, …, 32·3, 33·3,
2·5, 3·5, 4·5, …, 19·5, 20·5,
2·7, 3·7, 4·7, …, 13·7, 14·7,

余下的整数（不包括 1）就是所要求的不超过 $N=100$ 的素数.

我们将上述解答列表如下:

对于素数 $p_1=2,$

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

对于素数 $p_2 = 3,$

1 2 3 5 7 9
11 13 15 17 19
21 23 25 27 29
31 33 35 37 39
41 43 45 47 49
51 53 55 57 59
61 63 65 67 69
71 73 75 77 79
81 83 85 87 89
91 93 95 97 99

对于素数 $p_3 = 5,$

1 2 3 5 7
11 13 17 19
23 25 29
31 35 37
41 43 47 49
53 55 59
61 63 65 67
71 73 77 79
83 85 89
91 95 97

对于素数 $p_4 = 7,$

1 2 3 5 7
11 13 17 19
23 25 29
31 35 37
41 43 47 49
53 55 59

61 63 65 67
71 73 77 79
83 85 89
91 95 97

余下的整数（不包括1）就是所要求的不超过 $N=100$ 的素数:

1 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

素数为: $2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,61,67,71,73,79,83,89,97.$

1.1.4 欧几里德除法

因为不是任意的两个整数之间都有整除关系，所以我们需要引入欧几里德（Euclid）除法或带余数除法.

定理 1.1.11（欧几里德除法-最小非负余数） 设 a,b 是两个整数，其中 $b>0$. 则存在唯一的整数 q,r 使得

$$a=bq+r,\quad 0\le r<b \tag{1.1.2}$$

证（存在性）: 考虑一个整数序列

$$...,-3b,-2b,-b,0,b,2b,3b,...$$

它们将实数轴分成长度为 b 的区间，而 a 必定落在其中的一个区间中.

因此存在一个整数 q 使得 $qb\le a<(q+1)b$.

令 $r=a-bq$，则有 $a=bq+r,\quad 0\le r<b$.

（唯一性）: 如果分别有整数 q,r 和 q_1,r_1 满足（1.1.2），则

$$\begin{aligned} a&=bq+r, && 0\le r<b,\\ a&=bq_1+r_1, && 0\le r_1<b \end{aligned}.$$

两式相减，我们有 $b(q-q_1)=-(r-r_1)$.

当 $q\ne q_1$ 时，左边的绝对值大于等于 b，而右边的绝对值小于 b，这是不可能的.

故 $q=q_1,\quad r=r_1.$

定义 1.1.3 在 $a=bq+r,\quad 0\le r<b$ 式中，q 叫做 a 被 b 除所得的**不完全商**，r 叫做 a 被 b 除所得的**余数**.

因此，$b\mid a$ 的充要条件是 a 被 b 除所得的余数 $r=0$.

例 1.1.11 证明 $N=2027$ 为素数.

证 因为小于等于$\sqrt{2027}<46$的所有素数为 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 所以，依次用 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43 去试除:

2027 = 1013·2+1, 2027 = 675·3+2, 2027 = 405·5+2, 2027 = 289·7+4, 2027 = 184·11+3,
2027 = 155·13+12, 2027 = 119·17+4, 2027 = 106·19+13, 2027 = 88·23+3, 2027 = 69·29+26,
2027 = 65·31+12, 2027 = 54·37+29, 2027 = 49·41+18, 2027 = 47·43+6.

我们有 $2\nmid 2027, 3\nmid 2027, 5\nmid 2027$，$7\nmid 2027$，$11\nmid 2027$，$13\nmid 2027$，$17\nmid 2027$，$19\nmid 2027$，$23\nmid 2027$，$29\nmid 2027$，$31\nmid 2027$，$37\nmid 2027$，$41\nmid 2027$，$43\nmid 2027$，根据定理 **1.1.**9，$N=2027$ 为素数.

实际运用欧几里德除法时，我们可以根据需要，将余数取成其他形式.

定理 1.1.12 （欧几里德除法-一般余数） 设 a，b 是两个整数，其中 $b>0$. 则对任意的整数 c，存在唯一的整数 q，r 使得

$$a=bq+r,\qquad c\le r<b+c \tag{1.1.3}$$

证（存在性）：考虑一个整数序列

$$\ldots,-3b+c,-2b+c,-b+c,c,b+c,2b+c,3b+c,\ldots$$

它们将实数轴分成长度为 b 的区间，而 a 必定落在其中的一个区间中.

因此存在一个整数 q 使得 $qb+c\le a<(q+1)b+c$.

我们令 $r=a-bq$，则有 $a=bq+r, c\le r<b+c$.

（唯一性）：如果分别有整数 q, r 和 q_1, r_1 满足（1.1.3），则

$$a=bq+r, c\le r<b+c \qquad a=bq_1+r_1, c\le r_1<b+c.$$

两式相减，我们有 $b(q-q_1)=-(r-r_1)$.

当 $q\ne q_1$ 时，左边的绝对值大于等于 b，而右边的绝对值小于 b，这是不可能的.

故 $q=q_1, r=r_1$.

注:

1. 当 c=0 时，有 $0 \le r < b$，这时 r 叫做**最小非负余数.**

2. 当 c=1 时，有 $1 \le r < b+1$，这时 r 叫做**最小正余数.**

3. 当 c=-b+1 时，有 $-b+1 \le r < 0$，这时 r 叫做**最大非正余数.**

4. 当 c=- b 时，有 $-b \le r < 0$，这时 r 叫做**最大负余数.**

5. (i) 当 $b = 2k, c = -k$ 时，有 $-b/2 = -k \le r < k = b/2$，

(ii) 当 $b = 2k, c = -k+1$ 时，有 $-b/2 = -k < r \le k = b/2$，

(iii) 当 $b = 2k+1, c = -k$ 时，有 $-(b-1)/2 = -k \le r < k+1 = (b+1)/2$，或

$$-b/2 < -(b-1)/2 = -k \le r \le (b-1)/2 < b/2$$

总之，我们有 $-b/2 \le r < b/2$ 或 $-b/2 < r \le b/2$

这时，r 叫做**绝对值最小余数**.

例 1.1.12 设 b=7，则

余数 $r = 0,1,2,3,4,5,6$ 为最小非负余数.

余数 $r = 1,2,3,4,5,6,7$ 为最小正余数.

余数 $r = 0,-1,-2,-3,-4,-5,-6$ 为最大非正余数.

余数 $r = -1,-2,-3,-4,-5,-6,-7$ 为最大负余数.

余数 $r = -3,-2,-1,0,1,2,3$ 为绝对值最小余数.

例 1.1.13 设 b=12，则

余数 $r = 0,1,2,3,4,5,6,7$, 8, 9, 10, 11 为最小非负余数.

余数 $r = 1,2,3,4,5,6,7,8$, 9, 10, 11, 12 为最小正余数.

余数 $r = 0,-1,-2,-3,-4,-5,-6,-7$, -8, -9, -10, -11 为最大非正余数.

余数 $r = -1,-2,-3,-4,-5,-6,-7,-8$, -9, -10, -11, -12 为最大负余数.

余数 r = -6, -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5 或 r = -5, -4, -3, -2, -1, 0, 1, 2, 3, 4, 5, 6 为绝对值最小余数.

1.1.5 整数 b 进制表示

平时遇到的整数通常是以十进制表示. 例如 202409 意指 $2\cdot10^5 + 0\cdot10^4 + 2\cdot10^3 + 4\cdot10^2 + 0\cdot10^1 + 9\cdot10^0$. 中国是世界上最早采用十进制的国家，春秋战国时期已普遍使用的筹算就严格遵循了十进位制，见《孙子算经》. 但在计算机中，需要用二进制、八进制或十六进制表示整数. 为此, 我们考虑一般的 b 进制. 运用欧几里德除法, 我们可得到如下定理: .

定理 1.1.13 设 b 是大于 1 的正整数. 则每个正整数 n 可唯一地表示成

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 ,$$

其中 a_i 是整数， $0 \le a_i \le b-1, i = 1, ..., k,$ 且首项系数 $a_k \ne 0$.

证 (存在性)

用 b 去除 n 得到 $n = bq_0 + a_0, \quad 0 \le a_0 \le b-1.$

再用 b 去除不完全商 q_0， 得到 $q_0 = bq_1 + a_1, \quad 0 \le a_1 \le b-1.$

继续下去，依次得到

$$q_1 = bq_2 + a_2, \quad 0 \le a_2 \le b-1.$$

$$q_2 = bq_3 + a_3, \quad 0 \le a_3 \le b-1.$$

$$\cdots \cdots$$

$$q_{k-2} = bq_{k-1} + a_{k-1}, \quad 0 \le a_{k-1} \le b-1.$$

$$q_{k-1} = bq_k + a_k, \quad 0 \le a_k \le b-1.$$

因为 $0 \le q_k < q_{k-1} < \cdots < q_2 < q_1 < q_0 < n$. 所以, 必有整数 k, 使得不完全商 $q_k = 0$.

依此得到

$$n = bq_0 + a_0 .$$

$$n = b(bq_1 + a_1) + a_0 = b^2 q_1 + a_1 b + a_0 .$$

$$\cdots \cdots$$

$$n = b^{k-1} q_{k-2} + a_{k-2} b^{k-2} + \cdots + a_1 b + a_0 .$$

$$n = b^k q_{k-1} + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 .$$

$$= a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0 .$$

（唯一性） 如果有两种不同的表示式:

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0, \quad 0 \le a_i \le b-1, \quad i = 1, ..., k .$$

$$n = c_k b^k + c_{k-1} b^{k-1} + \cdots + c_1 b + c_0, \quad 0 \le c_i \le b-1, \quad i = 1, ..., k .$$

（这里可以取 $a_k = 0$ 或 $c_k = 0$.）两式相减得到

$$(a_k - c_k) b^k + (a_{k-1} - c_{k-1}) b^{k-1} + \cdots + (a_1 - c_1) b + (a_0 - c_0) = 0 .$$

假设 j 是最小的正整数使得 $a_j \ne c_j$， 则

$$b^j ((a_k - c_k) b^{k-j} + (a_{k-1} - c_{k-1}) b^{k-1-j} + \cdots + (a_{j+1} - c_{j+1}) b + (a_j - c_j)) = 0 .$$

或者 $(a_k - c_k) b^{k-j} + (a_{k-1} - c_{k-1}) b^{k-1-j} + \cdots + (a_{j+1} - c_{j+1}) b + (a_j - c_j) = 0 .$

因此， $a_j - c_j = -((a_k - c_k)b^{k-j-1} + (a_{k-1} - c_{k-1})b^{k-j-2} + \cdots + (a_{j+1} - c_{j+1}))b$.

故 $b \mid (a_j - c_j), \quad |a_j - c_j| \geq b$.

但 $0 \leq a_j \leq b-1, \quad 0 \leq c_j \leq b-1$ 有 $|a_j - c_j| < b$，这不可能.

因此，n 的表示式是唯一的.

为了更好地描述数学概念和问题，我们引入数学符号.

数学符号 $n = (a_k a_{k-1} \cdots a_1 a_0)_b$ **：** 如果展开式 $n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$，其中 a_i 是整数，$0 \leq a_i \leq b-1, i = 1, ..., k,$ 且首项系数 $a_k \neq 0$，则符号 $n = (a_k a_{k-1} \cdots a_1 a_0)_b$ 称为整数 n 的 ***b* 进制表示.**

当 $b = 2$，系数 a_i 为 0 或 1，因此我们有推论：

推论 1.1.3 每个正整数都可以表示成不同的 2 的幂的和.

例 1.1.**14 将**整数 404 表示为二进制.

解 逐次运用欧几里德除法，我们有

404=2·202+0, 202=2·101+0,

101=2·50+1, 50=2·25+0,

25=2·12+1, 12=2·6+0,

6=2·3+0, 3=2·1+1,

1=2·0+1.

因此, 404= $(110010100)_2$, 或者 $404 = 1 \cdot 2^8 + 1 \cdot 2^7 + 0 \cdot 2^6 + 0 \cdot 2^5 + 1 \cdot 2^4 + 0 \cdot 2^3 + 1 \cdot 2^2 + 0 \cdot 2^1 + 0 \cdot 2^0$.

计算机也常用八进制，或十六进制，或六十四进制等. 在十六进制中，我们用 0，1，2，3，4，5，6，7，8，9，A，B，C，D，E，F 分别表示 0，1，…，15 共 16 个数，其中 A，B，C，D，E，F 分别对应于 10，11，12，13，14，15.

例 1.1.**15** 转换十六进制 $(ABCD)_{16}$ 为十进制.

$$(ABCD)_{16} = 10 \cdot 16^3 + 11 \cdot 16^2 + 12 \cdot 16 + 13 = (43981)_{10}.$$

为了方便各进制之间的转换，并提高转换效率，我们可以预先制作一个换算表，再根据换算表作转换. 下图就是二进制、十进制和十六进制之间的换算表.

十进制	十六进制	二进制	十进制	十六进制	二进制
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

例 1.1.**16** 转换十六进制 $(ABCD)_{16}$ 为二进制.

解 由上述换算表可得 $A=(1010)_2, B=(1011)_2, C=(1100)_2, D=(1101)_2$. 从而 $(ABCD)_{16}=(1010101111001101)_2$.

例 1.1.**17** 转换二进制 $(110111101111)_2$ 为十六进制数.

解 由上述换算表可得到 $(1111)_2=F, (1110)_2=E, (1101)_2=D$,

从而 $(110111101111)_2=DEF$.

因为二进制的转换比十六进制要容易些，所以我们可以先将数作二进制表示，然后，运用二进制与十六进制之间的换算表，将二进制转换成十六进制.

例 1.1.**18** 表示整数 404 为十六进制.

解 根据例 1.1.14，我们有 $404=(110010100)_2$.

查换算表得到 $(0100)_2=4, (1001)_2=9, (0001)_2=1$.

故 $404=1\cdot16^2+9\cdot16+4=(194)_{16}$.

1.2 最大公因数 最小公倍数

我们不仅要讨论单个整数的因数，还要考虑多个整数的公共因数（简称公因数），特别是它们的最大公因数及其计算;在讨论公因数的同时,我们也将讨论公共倍数(简称公倍数)、最小公倍数及其基本性质。

1.2.1 最大公因数概念

定义 1.2.1 设 $a_1,...,a_n$ 是 $n\ (n\geq 2)$ 个整数. 若整数 d 是它们中每一个数的因数，那么 d 就叫做 $a_1,...,a_n$ 的一个**公因数**.

定义 1.2.2 设 d 是 $a_1,...,a_n$ 的一个公因数的数学表达式为 $d\mid a_1$， ...， $d\mid a_n$，如果整数 $a_1,...,a_n$ 不全为零，那么整数 $a_1,...,a_n$ 的所有公因数中最大的一个公因数叫做**最大公因数，**记作 $(a_1,...,a_n)$.

特别的，当 $(a_1,...,a_n)=1$ 时，我们称 $a_1,...,a_n$ **互素**或**互质.**

定理 1.2.1 设 $a_1,...,a_n$ 是 n 个不全为零的整数，则

（i） $a_1,...,a_n$ 与 $|a_1|,...,|a_n|$ 的公因数相同;

（ii） $(a_1,...,a_n)=(|a_1|,...,|a_n|)$.

证 （i）设 $d\mid a_i$， $1\leq i\leq n$，有 $d\mid |a_i|$， $1\leq i\leq n$． 故 $a_1,...,a_n$ 的公因数也是 $|a_1|,...,|a_n|$ 的公因数.

反之，设 $d\mid |a_i|$， $1\leq i\leq n$，同样有 $d\mid a_i$， $1\leq i\leq n$.故 $|a_1|,...,|a_n|$ 的公因数也是 $a_1,...,a_n$ 的公因数.

（ii）由（i）立得（ii）.

例 1.2.1 两个整数 25 和 35 的公因数为 $\{\pm 1,\pm 5\}$，它们的最大公因数 (25, 35)=5.

例 1.2.2 三个整数 6 和 25 和 35 的公因数为 $\{\pm 1\}$，它们的最大公因数 (6, 25, 35)=1.

或者说，三个整数 6 和 25 和 35 是互素的.

例 1.2.3 设 a,b 是两个整数，如果 $b\mid a$，且 $b>0$，则 $(a,b)=b$.

例 1.2.4 设 b 是任一正整数，则 $(0,b)=b$.

如：(1) (0, 6) = 6　　（2）(202409, 0) = 202409　　（3） $(0,b)=|b|$.

例 1.2.5 设 p 是一个素数，a 为整数. 如果 $p\nmid a$，则 p 与 a 互素.

证 设 $(p,a)=d$，则有 $d\mid p$ 及 $d\mid a$.

因为 p 是素数，所以由 $d\mid p$，我们有 $d=1$ 或 $d=p$.

对于 $d=p$，由 $d\mid a$，我们有 $p\mid a$，这与假设 $p\nmid a$ 矛盾.

因此，d=1，即 (p, a)=1，结论成立.

例 1.2.6 设 a,b 是两个整数，则我们有 $(a,b)=(a,-b)=(-a,b)=(|a|,|b|)$.

如：(25, 35)=(-25, 35)=(25, -35)=(-25, -35)=5.

定理 1.2.2 设 a,b,c 是三个不全为零的整数. 如果 $a=bq+c$，其中 q 是整数，则 $(a,b)=(b,c)$.

证 设 $d=(a,b),\ \ d'=(b,c)$，则 $d\mid a,\ \ d\mid b$. 由定理 **1.1.**3 知，$d\mid a+(-q)b=c,$ 因而，d 是 b，c 的公因数. 从而，$d\le d'$.

同理，d' 是 a，b 的公因数，$d'\le d$. 因此，$d=d'$.

例 1.2.7 因为 2409=6·365+219, 所以有 (202409, 365)=(365, 219).

因为 365=1·219+146, 所以有 (365, 219) = (219, 146)=73.

1.2.2 计算最大公因数-广义欧几里德除法

如何计算两个整数 a,b 的最大公因数？直接用最大公因数的定义，需要知道整数的因数分解式。当 a,b 是比较小的数时是可行的，但当 a,b 是很大数时，整数分解是很困难的问题. 为此，我们先给出一种算法——广义欧几里德除法或辗转相除法，然后运用它求 a,b 的最大公因数.

定义 1.2.3 (广义欧几里德除法) 设 a,b 是任意两个正整数，记 $r_0=a,\ \ r_1=b$. 反复运用欧几里德除法，我们有

$$\begin{aligned} r_0&=r_1q_1+r_2, && 0\le r_2<r_1,\\ r_1&=r_2q_2+r_3, && 0\le r_3<r_2,\\ &\cdots && \cdots\\ r_{n-2}&=r_{n-1}q_{n-1}+r_n, && 0\le r_n<r_{n-1},\\ r_{n-1}&=r_nq_n+r_{n+1}, && r_{n+1}=0. \end{aligned} \tag{1.2.1}$$

经过有限步骤，必然存在 n 使得 $r_{n+1}=0$，这是因为

$$0=r_{n+1}<r_n<r_{n-1}<\cdots<r_2<r_1=b \qquad \text{且 } b \text{ 是有限正整数.}$$

定理 1.2.3 设 a,b 是任意两个正整数，则 $(a,b)=r_n$，其中 r_n 是广义欧几里德除法 (1.2.1) 中最后一个非零余数.

证 根据定理 1.2.2，有

$$\begin{aligned}(a,b)&=(b,r_2)\\&=(r_2,r_3)\\&=\cdots\\&=(r_{n-1},r_n)\\&=(r_n,0)\end{aligned}$$

所以有 $(a,b)=(r_n,0)=r_n$. 因此，结论成立.

因为求两个整数的最大公因数在信息安全的实践中起着重要的作用，所以我们将求两个整数的最大公因数之过程详解如下.

首先，根据定理 1.2.1，将求两个整数的最大公因数转化为求两个非负整数的最大公因数;

其次，运用欧几里德除法，并根据定理 1.2.3，我们可以将求两个正整数的最大公因数转化为求两个较小的非负整数的最大公因数;

再次，反复运用欧几里德除法，即广义欧几里德除法，来将求两个正整数的最大公因数转化为求 0 和一个正整数的最大公因数;

最后，根据定理 1.2.3，求出两个整数的最大公因数.

例 1.2.8 设 a = 377, b = 221, 计算 (a,b).

解 利用广义欧几里德除法，有

377 = 1·221+156, 221 = 1·156+65, 156 = 2·65+26, 65 = 2·26+13, 26 = 2·13,

所以, (377, 221) =13.

例 1.2.9 设 a = 518860799, b = 259339331, 计算 (a,b).

解 利用广义欧几里德除法,

方法一：最小非负余数.

518860799 = 2·259339331+182137, 259339331 = 1423·182137+158380,

182137 = 1·158380+23757, 158380 = 6·23757+15838,

23757 = 1·15838+7919, 15838 = 2·7919.

方法二：绝对值最小余数.

518860799 = 2·259339331+182137, 259339331 = 1424·182137-23757,

182137 = 8·23757-7919, 23757 = 3·7919.

所以, (518860799, 259339331) = 7919.

1.2.3 贝祖（B*ézout*）等式

从广义欧几里德除法的算式中，我们观察到

$$r_n = r_{n-2} - r_{n-1}q_{n-1}$$

$$r_{n-1} = r_{n-3} - r_{n-2}q_{n-2}$$

……

$$r_3 = r_1 - r_2 q_2$$

$$r_2 = r_0 - r_1 q_1$$

通过逐次消去 $r_{n-1}, r_{n-2}, \cdots\cdots r_3, r_2,$ 可以找到整数 s,t，使得 $sa+tb=(a,b)$.

定理 1.2.4 设 a，b 是任意两个正整数，则存在整数是 s，t 使得

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

成立，该式叫做**贝祖等式**.

根据广义欧几里德的逆向运算，可以得到贝祖等式的结论. 此外，还有其余的证明贝祖等式的方法，有兴趣的读者可以参考课外资料.

例 1.2.10 设 a = 377, b = 221，求整数 s，t，使得 $sa+tb=(a,b)$.

解 由例 1.2.8，我们有

$$\begin{aligned} 13 &= 65\text{-}2\cdot 26 \\ &= 65\text{-}2\cdot(156\text{-}2\cdot 65) \\ &= 5\cdot 65\text{-}2\cdot 156 \\ &= 5\cdot(221\text{-}1\cdot 156)\text{-}\ 2\cdot 156 \\ &= 5\cdot 221\text{-}7\cdot 156 \\ &= 5\cdot 221\text{-}7\cdot(337\text{-}1\cdot 221) \\ &= 12\cdot 221\text{-}7\cdot 337 \end{aligned}$$

因此，整数 s = -7, t = 12 满足 $sa+tb=(a,b)$.

例 1.2.11 设 a = 518860799, b = 259339331，求整数 s，t，使得 $sa+tb=(a,b)$.

解 由例 1.2.9，根据最小非负余数，我们有

$$\begin{aligned} 7919 &= 23757\text{-}1\cdot 15838 \\ &= 23757\text{-}1\cdot(158380\text{-}6\cdot 23757) \\ &= 7\cdot 23757\text{-}1\cdot 158380 \\ &= 7\cdot(182137\text{-}1\cdot 158380)\text{-}1\cdot 158380 \\ &= 7\cdot 182137\text{-}8\cdot 158380 \\ &= 7\cdot 182137\text{-}8\cdot(259339331\text{-}1423\cdot 182137) \\ &= 11391\cdot 182137\text{-}8\cdot 259339331 \end{aligned}$$

= 11391·(518860799-2·259339331)-8·259339331

= 11391·518860799-22790·259339331

因此，整数 s = 11391, t = -22790 满足 $sa+tb=(a,b)$.

定理 1.2.5 整数 a，b 互素的充分必要条件是存在整数 s,t 使得 $sa+tb=1$.

证 根据定理 1.2.4，我们立即得到命题的必要性成立.

反过来，

设 $d=(a,b)$，则有 $d\mid a,\quad d\mid b$. 现在若存在正整数 s,t 使得

$$sa+tb=1,$$

则我们有 $d\mid sa+tb=1.$

因此，$d=1$，即整数 a，b 互素.

例 1.2.12 设四个整数 a，b，c，d 满足关系式：$ad-bc=1$

则 $(a,b)=1,\ (a,c)=1,\ (d,b)=1,\ (d,c)=1.$

1.2.4 最大公因数性质

下面，给出最大公因数定义的数学表述形式.

定理 1.2.6 设 a，b 是任意两个不全为零的整数，d 是正整数，则 d 是整数 a，b 的最大公因数的充要条件是:

(i) $d\mid a,\ d\mid b$;

(ii) $e\mid a,\ e\mid b,$ 则$e\mid d.$

证 若 d 是整数 a，b 的最大公因数，则显然有 (i) 成立;

由定理 1.2.4，存在整数 s，t 使得 $sa+tb=d$.

因此，当 $e\mid a,\ e\mid b$ 时，有 $e\mid sa+tb=d$.

故 (ii) 成立.

反过来，假设 (i) 和 (ii) 成立，

那么 (i) 说明 d 是整数 a，b 的公因数;

(ii) 说明 d 是整数 a，b 的公因数中的最大数，因为 $e\mid d$ 时，有 $|e|\le d$.

因此，d 是整数 a，b 的最大公因数.

定理 1.2.7 设 a，b 是两个不全为零的整数，

(i) 若 m 是任一正整数，则 $(am,\ bm)=(a,\ b)m$.

(ii) 若非零整数 d 满足 $d\mid a,\ d\mid b$ 则 $(\frac{a}{d},\ \frac{b}{d})=\frac{(a,\ b)}{|d|}$.

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

证：先证明 (i)

设 $d=(a,b),\quad d'=(am,bm)$.

由广义欧几里德除法，存在整数 s，t 使得 $sa+tb=d$.

两端同乘 m，得到 $s(am)+t(bm)=dm$.

因此 $d'\mid dm$.（即$\because d'=(am,bm)$，有 $dm\mid am,\quad dm\mid bm$，有 $dm\mid am+bm$）.

又显然有 $dm\mid am,\quad dm\mid bm$.

根据 d' 是最大公因数，$d'=(am,bm)$，有 $dm\mid d'$.

故 $d'=(am,bm)=dm$ 即 (i) 成立.

再证明 (ii)

根据结论 (i)，当 $d\mid a,\ d\mid b$ 时，我们有

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

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

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

故 (ii) 成立.

例 1.2.13 设 $a=11\cdot202409$, b $=23\cdot202409$, 计算 (a,b).

解 因为 $(11,\ 23)=(11,\ 23-11\cdot2)=(11,\ 1)=1$.

所以 $(a,\ b)=(11\cdot202409,\ 23\cdot202409)=202409$.

定理 1.2.8 设 a，b，c 是三个整数，且 $b\neq0,\quad c\neq0,$ 如果 $(a,c)=1$，则

$$(ab,\ \ c)=(b,\ \ c).$$

证 令 $d=(ab,c),\quad d'=(b,c)$.

根据d'是 b 与 c 最大公因数，有$d'|b,\ \ d'|c,$

进而$d'|ab,\ d'|c,$ 即d'是 ab 与 c 的公因数

由于 d 是 ab 与 c 的最大公因数.

我们得到$d'|d$.

反过来，因为$(a,c)=1$,

根据广义欧几里德除法存在整数 s，t 使得$sa+tc=1$.

两端同乘 b，得到$s(ab)+(tb)c=b$.

由于 d 是 ab 与 c 的最大公因数，有$d|ab,\ d|c,$

我们得到$d|s(ab)+(td)c,$ 即$d|b.$，即 d 是 b 与 c 的公因数

由于d'是 b 与 c 的最大公因数,

我们得到$d|d'$.

故$d=d'$.

推论 1.2.1 设$n-1$ $(n\geq 3)$ 为整数，如果$(a_i,c)=1,\ \ 1\leq i\leq n,$ 则

$$(a_1\cdots a_n,\ c)=1.$$

证 我们对 n 作数学归纳法.

n=2 时，由定理 1.2.8 易得.

假设 n-1 时，命题成立. 即 $(a_1\cdots a_{n-1},\ c)=1$.

对于 n，根据归纳假设，我们有$(a_1\cdots a_{n-1},\ c)=1$,

再根据$(a_n,\ c)=1$及定理 1.2.8,

我们得到 $(a_1\cdots a_{n-1}a_n,\ c)=1=((a_1\cdots a_{n-1})a_n,\ c)$

因此，命题对所有的 n 成立.

前面我们讨论了如何求两个整数的最大公因数. 对于 n 个整数$a_1,\cdots,a_n$的最大公因数，我们可以用递归的方法，将求它们的最大公因数转化为一系列求两个整数的最大公因数. 具体过程如下:

推论 1.2.2 设$a_1,\cdots,a_n$是 n 个整数，且$a_1\neq 0$. 令$(a_1,a_2)=d_2,\ \ \cdots,(d_{n-1},a_n)=d_n$，则$(a_1,\cdots,a_n)=d_n$.

例 1.2.14 计算最大公因数 (12, 25, 100, 256).

解 因为

$$(12, 25) = 1,$$
$$(1, 100) = 1,$$
$$(1, 256) = 1,$$

所以最大公因数 $(12, 25, 100, 256) = 1$.

推论 1.2.3 设 $a_1, \cdots, a_n$ 是任意 n 个不全为零的整数，则 d 是最大公因数的充要条件是:

(*i*) $d \mid a_1, \ldots, \quad d \mid a_n$

(*ii*) 若 $e \mid a_1, \ldots, \quad e \mid a_n$，则 $e \mid d$

证 该证明思路与过程，同定理 1.2.6 类似.

定理 1.2.9 设 a，b，c 是三个整数， 且 $c \neq 0$. 如果 $c \mid ab, \quad (a,c) = 1,$，则 $c \mid b.$

证 根据假设条件和定理 1.2.8,

我们有 $c \mid (ab,\ c) = (b,c)$,

从而 $c \mid b.$

定理 1.2.10 设 p 是素数，若 $p \mid ab$，则 $p \mid a$ 或 $p \mid b$.

证 若 $p \nmid a$，已知 p 是素数，有 $(p,a) = 1.$

再由 $p \mid ab$，根据定理 1.2.9，我们有 $p \mid b$.

从而，命题成立.

推论 1.2.4 设 $a_1, \cdots, a_n$ 是 n 个整数，p 是素数，若 $p \mid a_1 \cdots a_n$， 则 p 一定整除某一个 a_k.

证 若 $a_1, \cdots, a_n$ 都不能被 p 整除,

由已知 p 是素数，有 $(a_i, p) = 1, \quad 1 \le i \le n$

而 $(a_1 \cdots a_n, p) = 1$. 这与 $p \mid a_1 \cdots a_n$ 矛盾，所以结论正确.

例 1.2.15 因为 365|12·2555, 又(365, 12) = 1, 所以 365|2555.

例 1.2.16 因为 7|5·2555，又 7∤5及 7 为素数，所以 7|2555.

1.2.5 最小公倍数及性质

定义 1.2.4 设 $a_1,\cdots,a_n$ 是 n 个整数，若 m 是这 n 个数的倍数，则 m 叫做这 n 个数的一个**公倍数**. $a_1,\cdots,a_n$ 的所有公倍数中的最小正整数叫做**最小公倍数**，记作 $[a_1,\cdots,a_n]$.

定理 1.2.11 设 a，b 是两个互素正整数，则，

(i) 若 $a|m$，$b|m$，则 $ab|m$.

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

证 (i) 设 $a|m$，则 $m=ak$.

又 $b|m$，即 $b|ak$，

以及 $(a,b)=1$，根据定理 1.2.9，得到 $b|k$.

因此：$k=bt$，$m=abt$. 故 $ab|m$. (i) 得证.

(ii) 显然 ab 是 a，b 的公倍数.

又由(i)知，ab 是 a，b 的公倍数中最小正整数， 故 $[a,b]=ab$.

例 1.2.17 整数 14 和 21 的公倍数为 $\{\pm 42, \pm 84, \cdots\}$，最小公倍数为 $[14,21]=42$.

例 1.2.18 设 p，q 是两个不同的素数，则 $[p,q]=pq$.

定理 1.2.12 设 a，b 是两个正整数，则

(i) 若 $a\mid m, b\mid m$, 则 $[a,b]\mid m$;

(ii) $[a,b]=\dfrac{ab}{(a,b)}$.

证 令 $d=(a,b)$，根据定理 1.2.7，我们有

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

又根据定理 1.2.11

$$\left[\frac{a}{d},\frac{b}{d}\right]=\frac{a}{d}\cdot\frac{b}{d}$$

进而 $\left[a,b\right]=\dfrac{ab}{d}$，即(ii)成立.

再由

$$\frac{a}{d}\mid\frac{m}{d},\quad \frac{b}{d}\mid\frac{m}{d}$$

得到

$$\frac{a}{d}\cdot\frac{b}{d}\mid\frac{m}{d}$$

从而 $\frac{ab}{d}\mid m$，即(i)成立.

对于 n 个整数 $a_1,\cdots,a_n$ 的最小公倍数，我们可以用递归的方法，将求它们的最小公倍数转化为一系列求两个整数的最小公倍数. 具体过程如下:

定理 1.2.13 设 $a_1,\cdots,a_n$ 是 n 个整数. 令

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

则 $[a_1,\cdots,a_n]=m_n$.

例 1.2.19 计算最小公倍数 [12, 25, 100, 256].

解 因为

$$[12,25]=\frac{12\cdot 25}{(12,25)}=300,$$

$$[300,100]=\frac{300\cdot 100}{(300,100)}=\frac{300\cdot 100}{100}=300,$$

$$[300,256]=\frac{300\cdot 256}{(300,256)}=\frac{300\cdot 256}{4}=19200.$$

所以最小公倍数 [12, 25, 100, 256] = 19200.

定理 1.2.14 设 $a_1,\ a_2,\ \cdots,\ a_n$ 是正整数，如果 $a_1\mid m,\ \ a_2\mid m,\ \ \cdots,\ \ a_n\mid m,$

则 $[a_1,\ \cdots,\ a_n]\mid m$.

证 对 n 作数学归纳法.

n=2 时，命题就是定理 1.2.12 (i).

假设 $n-1\ \ (n\geq 3)$ 时，命题成立. 即

$$m_{n-1}=[a_1,a_2,\cdots,a_{n-1}]\mid m$$

对于 n，根据归纳假设，我们有 $m_{n-1}\mid m$.

再根据定理 1.2.13，$[m_{n-1},a_n]=[a_1,a_2,\cdots,a_n]$，我们得到

$$[a_1,a_2,\cdots,a_n]\mid m.$$

因此，命题对所有的 n 成立.

1.3 整数分解

整数分解，是数学中的一个重要概念，简单来说就是将一个正整数写成其因数的乘积. 这个过程在数学、计算机科学、密码学等多个领域都有广泛的应用. 本节给出一个简单的整数分解方法，同时给出关于整数分解的一个理论性基础结果.

1.3.1 整数分解定理

定理 1.3.1（**整数分解定理**） 给定正合数 $n>1$. 如果存在整数 a, b 使得 $n \mid a^2-b^2, n \nmid a-b, n \nmid a+b$, 则 $(n, a-b)$ 和 $(n, a+b)$ 都是 n 的真因数.

证 若 $(n, a-b)$ 不是 n 的真因数，则 $(n, a-b)$ 为 1 或 n. 对于 $(n, a-b)=1$，由 $n \mid a^2-b^2$ 而 $a^2-b^2=(a-b)(a+b)$ 得 $n \mid a+b$, 与题设矛盾. 对于 $(n, a-b)=n$, 推出 $n \mid a-b$, 与题设矛盾. 故 $(n, a-b)$ 是 n 的真因数.

同理, $(n, a+b)$ 也是 n 的真因数.

1.3.2 素数的算术基本定理

我们在前面讨论过素数，并证明了每个整数都有一个素因数. 下面我们要证明每个整数一定可以表示成素数的乘积，并且该表达式是唯一的（在不考虑乘积顺序的情况下）.

定理 1.3.2（**算术基本定理**） 任一整数 $n>1$ 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

$$n=p_1 \cdots p_s, \quad p_1 \leq \cdots \leq p_s \tag{1.3.1}$$

其中 p_i 是素数，并且若

$$n=q_1 \cdots q_t, \quad q_1 \leq \cdots \leq q_t$$

其中 q_i 是素数，则 $s=t, \quad p_i=q_i, \quad 1 \leq i \leq s$.

证 首先用数学归纳法证明：任一整数 $n>1$ 都可以表示成素数的乘积，即（1.3.1）式成立.

$n=2$，（1.3.1）式显然成立.

假设对于小于 n 的正整数，（1.3.1）式成立.

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 使得

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

根据归纳假设,

$$b=p_1' \cdots p_u', \quad c=p_{u+1}' \cdots p_s'$$

于是，

$$n = p_1' \cdots p_s'$$

适当改变 p_i' 的次序即得(1.3.1)式，故（1.3.1）式对于 n 成立.

综上，根据数学归纳法原理，（1.3.1）式对于所有 $n>1$ 的整数成立.

再证明表达式是唯一的，设还有

$$n = q_1 \cdots q_t, \quad q_1 \le \cdots \le q_t$$

其中 q_j 是素数，则

$$p_1 \cdots p_s = q_1 \cdots q_t \tag{1.3.2}$$

因此 $p_1 \mid q_1 \cdots q_t$,

由于 p_1 是素数，根据推论 1.2.4，存在 q_j 使得 $p_1 \mid q_j$,

但 p_1，q_j 都是素数，故 $p_1 = q_j$.

同理，存在 p_k 使得 $q_1 = p_k$ ，这样

$$p_1 \le p_k = q_1 \le q_j = p_1$$

进而 $p_1 = q_1$. 将（1.3.2）式两端同时消除 p_1 ，我们有

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

同理，可推出 $p_2 = q_2$.

以此类推，依次得到

$$p_3 = q_3, \ \cdots, \ q_s = p_t \quad \text{以及 } s=t.$$

例 1.3.1 写出整数 12, 25, 100, 256 的因数分解式.

解 根据定理 1.3.2，我们有

$$12 = 2\cdot 2\cdot 3, \qquad 25 = 5\cdot 5,$$
$$100 = 2\cdot 2\cdot 5\cdot 5, \quad 256 = 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2\cdot 2.$$

将相同的素数乘积写成素数幂的形式，定理 1.3.2 可表述为：

定理 1.3.3 任一整数 $n>1$ 可唯一的表示成

$$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \qquad \alpha_i > 0, \ \ i = 1, \cdots, s \tag{1.3.3}$$

其中 $p_i < p_j \quad (i < j)$ 是素数. 这里，（1.3.3）式叫做 n 的**标准分解式.**

例 1.3.2 写出整数 12, 25, 100, 256 的标准分解式.

解 根据定理 1.3.2 和例 1.3.1，我们有

$$12 = 2^2 \cdot 3, \qquad 25 = 5^2,$$
$$100 = 2^2 \cdot 5^2, \qquad 256 = 2^8.$$

在应用中，为了方便，整数的因数分解式常写成

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

定理 1.3.4 设 n 是大于 1 的一个整数，且有标准分解式：

$$n = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \quad \alpha_i > 0, \quad i = 1, \cdots, s. \tag{1.3.4}$$

则 d 是 n 的正因数，当且仅当 d 有因数分解式

$$d = p_1^{\beta_1} \cdots p_s^{\beta_s}, \quad \alpha_i \geq \beta_i \geq 0, i = 1, \cdots, s.$$

证 设 $d|n$，且 d 有因式分解式：

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

则我们一定有

$$\alpha_i \geq \beta_i, \quad i = 1, \cdots, s$$

否则，存在$1 \leq i \leq s$，使得$\alpha_i < \beta_i$. 不妨设$\alpha_1 < \beta_1$.根据 $d|n$ 及 $p_1^{\beta_1} \mid d$，

我们有

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

两端消除 $p_1^{\alpha_1}$，得到

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

再根据推论 1.2.4，存在 j，$2 \leq j \leq s$ 使得

$$p_1 \mid p_j$$

这不可能. 故（1.3.4）式成立.

反过来，若（1.3.4）式成立，则

$$n' = p_1^{\alpha_1 - \beta_1} \cdots p_s^{\alpha_s - \beta_s}$$

是一个整数，且使得

$$n = dn'$$

这说明$d \mid n$.

例 1.3.3 设正整数 n 有因式分解式

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

则 n 的因数个数

$$d(n) = (1+\alpha_1) \cdots (1+\alpha_s) \ .$$

证 设 $d|n$，且 d 有因数分解式:

$$d = p_1^{\beta_1} \cdots p_s^{\beta_s}, \quad \alpha_i \geq \beta_i \geq 0, \quad i = 1, \cdots, s$$

因为 β_1 的变化范围是从 0 到 α_1 共 $1+\alpha_1$ 个值，…，

β_s 的变化范围是 0 到 α_s 共 $1+\alpha_s$ 个值.

所以 n 的因数个数为

$$d(n) = (1+\alpha_1) \cdots (1+\alpha_s) \ .$$

定理 1.3.5 设 a，b 是两个正整数，且都有标准分解式:

$$a = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \quad \alpha_i \geq 0, i = 1, \cdots, s$$
$$b = p_1^{\beta_1} \cdots p_s^{\beta_s}, \quad \beta_i \geq 0, i = 1, \cdots, s$$

则 a 和 b 的最大公因数和最小公倍数分别有有因数分解式:

$$(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_s^{\min(\alpha_s,\beta_s)}$$
$$[a,b] = p_1^{\max(\alpha_1,\beta_1)} \cdots p_s^{\max(\alpha_s,\beta_s)} .$$

证 根据定理 1.3.4，我们知道整数

$$d = p_1^{\min(\alpha_1,\beta_1)} \cdots p_s^{\min(\alpha_s,\beta_s)} .$$

满足最大公因数的数学定义，

所以

$$(a,b) = p_1^{\min(\alpha_1,\beta_1)} \cdots p_s^{\min(\alpha_s,\beta_s)} .$$

同样，整数

$$m = p_1^{\max(\alpha_1,\beta_1)} \cdots p_s^{\max(\alpha_s,\beta_s)} .$$

满足最小公倍数的数学定义，

所以

$$[a,b] = p_1^{\max(\alpha_1,\beta_1)} \cdots p_s^{\max(\alpha_s,\beta_s)} .$$

推论 1.3.1 设 a，b 是两个正整数，则

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

证 对任意整数 $\alpha, \beta,$ 我们有

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

根据定理 1.3.5，结论成立.

例 1.3.4 计算整数 12, 25, 100, 256 的最大公因数和最小公倍数.

解 根据定理 1.3.2，我们有

$$12 = 2^2\cdot 3, \qquad 25 = 5^2,$$
$$100 = 2^2\cdot 5^2, \qquad 256 = 2^8.$$

再根据定理 1.3.5，我们有

$$(12, 25) = 1, (1, 100) = 1, (1, 256) = 1.$$

所以整数 12, 25, 100, 256 的最大公因数为 1.

同样，根据定理 1.3.5，我们有

$$[12, 25] = 2^2\cdot 3\cdot 5^2 = 300,$$
$$[300, 100] = 2^2\cdot 3\cdot 5^2 = 300,$$
$$[300, 256] = 2^8\cdot 3\cdot 5^2 = 19200.$$

所以整数 12, 25, 100, 256 的最小公倍数为 19200.

利用整数的唯一因数分解式，我们给出如下结果. 该结果将用于原根的构造.

例 1.3.5 设 a，b 是两个正整数，则存在整数 $a'\mid a,\ b'\mid b$ 使得

$$a'\cdot b' = [a,b], \quad (a', b') = 1.$$

证 设整数 a，b 有如下的因数分解式:

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

其中 $\alpha_i \ge \beta_i \ge 0, (i = 1,\cdots,t); \beta_i \ge \alpha_i \ge 0, (i = t+1,\cdots,s)$.

我们取

$$a' = p_1^{\alpha_1}\cdots p_t^{\alpha_t}, \quad b' = p_{t+1}^{\beta_{t+1}}\cdots p_s^{\beta_s}$$

则整数 a', b' 即为所求.

例 1.3.6 设 $a = 2^2\cdot 3^3\cdot 5^4\cdot 7^5\cdot 11^6$, $b = 2^6\cdot 3^5\cdot 5^4\cdot 7^3\cdot 11^2$.

我们取

$$a' = 2^6\cdot 3^5\cdot 5^4,\ b' = 7^5\cdot 11^6.$$

则有

$$a'\cdot b' = 2^6\cdot 3^5\cdot 5^4\cdot 7^5\cdot 11^6 = [a, b].$$

习题

1. 证明:若$2|n,3|n,5|n$,则$30|n$.
2. 证明:若a是整数,则$3|a^3-a$.
3. 证明:任意三个连续的整数的乘积都能被6整除.
4. 利用 Eratosthenes 筛法求出 150 以内的所有素数,要求给出计算过程.
5. 有一个六位数，一、四位，二、五位，三、六位的数字相同，试证明此数可以被 7、11、13 整除.
6. 问是否存在这样的整数a,b,c,使得$a|bc$,但$a\nmid b,a\nmid c$,举两例说明,若无,给出证明.
7. 证明：由$p\mid 10a-b$和$p\mid 10c-d$，可得$p\mid ad-bc$.
8. 证明：任何不能被 3 整除的自然数的平方，用 3 除时余 1.
9. 有一个 2024 位的数 A 能被 9 整除，它的各位数字和为 a，a 的各位数字和为 b，b 的各位数字和为 c，求 c 等于多少？
10. 一个正整数，它的平方壳表示成一个正的二位整数与这二位数字倒过来写成的二位之和，求这个正整数.
11. 证明：若三个大于 10 的素数成等差数列，其公差为 d，则 6 ｜ d.
12. 求方程$1!+2!+3!+\ \ldots\ldots+n!=m^2$的整数解.
13. 证明:对于任意给定的正整数k,必有连续k个正整数都是合数.
14. 利用广义欧几里德除法计算两个整数$a=2394,b=5567$的最大公约数(a,b),并求出整数s,t,使得$(a,b)=sa+tb$.
15. 计算$[2394,5567]$.
16. 计算(435785667，131901878).
17. 证明:$\big((a,b),b\big)=(a,b)$.
18. 两个正整数的差为 21，最小公倍数为 70，求这两个数.
19. 求以下整数对的最大公因数、最小公倍数.
(i) $(2n+1,2n-1)$
(ii) $(2n,2(n+1))$
20. 两个正整数的最大公因数为 9，最小公倍数为 135，求这两个数。
21. 求下列各数的标准分解式：
(i)20520
(ii)9699690
22. 用分解素因数的方法求最大公因数：
(i)56，210，378
(ii)63，240，384
23. 利用因子分解定理求解整数420,192,450,969的最大公因子与最小公倍数.
24. 设a,b为正整数,证明:若$[a,b]=(a,b)$,则$a=b$.
25. 设n为合数,证明n必有素因子p满足$p\le\sqrt{n}$.