第一章

整数的可除性

数论的基本研究对象是整数, 而整除理论是数论之基础. 本章的主要结果为数论中最基本、最重要的定理之一——算术基本定理. 围绕这一定理, 第一节建立整除理论中最重要的工具: 带余除法, 并介绍其若干应用. 第二节通过辗转相除法建立最大公因子与最小公倍数理论, 证明 Bézout 定理, 并给出最大公因子的有效算法. 作为 Bézout 定理的应用, 第三节建立一次不定方程理论. 第四节证明算术基本定理, 并研究素数的分布与判定问题.

1.1　带余除法

1.1.1　带余除法

在整数集 $\mathbb{Z}$ 上可以定义加法、减法、乘法运算, 并且加法和乘法运算满足交换律与结合律, 乘法对加法满足分配律. 然而两个整数之商未必是整数, 为此我们引入带余除法.

定理 1.1.1　给定两个整数 a 和 b, 其中 $b>0$, 存在唯一的一对整数 q 和 r, 使得

$$a=qb+r \quad \text{且} \quad 0\leqslant r<b.$$

证明　令

$$S=\{a-nb \mid n\in\mathbb{Z}\}.$$

则 $S\cap\mathbb{N}$ 为 $\mathbb{N}$ 的非空子集, 这是因为 S 中包含自然数 $a+|a|b$ (取 $n=-|a|$). 根据最小自然数原理, $S\cap\mathbb{N}$ 有最小元素 $r=a-qb$, 其中 $q\in\mathbb{Z}$. 若 $r\geqslant b$, 则 S 中包含自然数 $a-(q+1)b=r-b$. 但这和 r 的最小性矛盾, 因此 $0\leqslant r<b$. 这就证明了 q 和 r 的存在性.

设有整数 q' 和 r' 也满足

$$a=q'b+r' \quad \text{且} \quad 0\leqslant r'<b.$$

则 $r-r'=(q'-q)b$. 若 $q\neq q'$, 则 $|r-r'|=|q'-q|b\geqslant b$. 这和 $0\leqslant r<b$ 与 $0\leqslant r'<b$ 矛盾, 故 $q=q'$ 且 $r=r'$. 这就证明了 q 和 r 的唯一性. □

定义1.1.1　定理 1.1.1 中的 q 称为 a 除以 b 的**不完全商**, r 为 a 除以 b 的**余数**.

定理 1.1.1 有如下简单推论:

推论1.1.1　设 a,b 是两个整数, 其中 $b\neq0$, 存在唯一的一对整数 q 和 r, 使得

$$a=qb+r \quad \text{且} \quad 0\leqslant r<|b|.$$

例1.1.1　设 n 是整数, 证明 n^2 除以 4 的余数为 0 或 1.

证明 若 n 为奇数, 取整数 k 使得 $n=2k+1$. 此时, $n^2=(2k+1)^2=4(k^2+k)+1$ 除以 4 的余数为 1.

若 n 为偶数, 取整数 l 使得 $n=2l$. 此时, $n^2=4l^2$ 除以 4 的余数为 0.

1.1.2 整除

定义1.1.2 设 a,b 是两个整数. 若存在整数 c 使得 $a=bc$, 则称 b 是 a 的**因子**, a 是 b 的**倍数**, 或者 b **整除** a, 或者 a 能被 b 整除; 否则称为 b **不整除** a. 我们用记号 $b\mid a$ 表示 b 整除 a, $b\nmid a$ 表示 b 不整除 a.

命题1.1.1 (1) $a\mid b\iff -a\mid b\iff a\mid(-b)\iff |a|\mid|b|$;

(2) (传递性) $a\mid b$ 且 $b\mid c\Longrightarrow a\mid c$;

(3) (可加性) $a\mid b_1,a\mid b_2,\cdots,a\mid b_k\iff$ 对任何 $x_1,x_2,\cdots,x_k\in\mathbb{Z}$ 都有 $a\mid x_1b_1+x_2b_2+\cdots+x_kb_k$;

(4) (自反性) $a\mid b$ 且 $b\mid a\iff a=\pm b$;

(5) 若整数 $m\neq 0$, 则 $a\mid b\iff ma\mid mb$;

(6) 若 $b\neq 0$, 则 $a\mid b\Longrightarrow |a|\leqslant|b|$.

证明 (1), (2), (5) 和 (6) 显然, 只证 (3) 和 (4).

(3) 假设对任何 $1\leqslant i\leqslant k$ 都有 $a\mid b_i$. 根据定义存在整数 u_i 使得 $b_i=u_ia$, 于是 $x_1b_1+x_2b_2+\cdots+x_kb_k=(x_1u_1+x_2u_2+\cdots+x_ku_k)a$, 必要性得证. 反之, 假设对任何整数 $x_1,x_2,\cdots,x_k$ 都有 $a\mid x_1b_1+x_2b_2+\cdots+x_kb_k$. 特别地, 固定 $1\leqslant i\leqslant k$, 对任何 $1\leqslant j\leqslant k$, 取 $x_j=\delta_{ij}$, 有 $a\mid b_i$, 充分性得证.

(4) 充分性显然. 对必要性, 假设 $a\mid b$ 且 $b\mid a$. 于是存在整数 p,q 使得 $b=pa$, $a=qb$. 若 $a=0$, 则 $b=pa=0=a$. 若 $a\neq 0$, 则 $a=qb=(qp)a$. 从而 $q=\pm1$ 且 $a=\pm b$. □

1.2 最大公因子与最小公倍数

上一节介绍了整除与因子, 这一节研究两个整数的公因子.

1.2.1 最大公因子

定义1.2.1 设 a,b 是两个整数. 如果整数 d 同时满足 $d\mid a$ 和 $d\mid b$, 则称 d 是 a 和 b 的**公因子**.

定义1.2.2　两个整数 a 和 b 的**最大公因子**定义为满足下列条件的唯一整数 d:

(1) $d \mid a$ 且 $d \mid b$,

(2) 若 $c \mid a$ 且 $c \mid b$, 则 $c \leqslant d$.

注记1.2.1　(1) 当 $a = b = 0$ 时, 所有整数都是 a, b 的公因子, 此时 a, b 不存在最大公因子.

(2) 当 a, b 不全为零时, 由命题 1.1.1 (6) 知 a, b 的公因子 d 必满足 $d \leqslant \max\{|a|, |b|\}$. 此时, a, b 的最大公因子存在, 并且为它们所有公因子中最大的那个, 我们用记号 $\gcd(a, b)$ 表示 a 和 b 的最大公因子.

命题1.2.1　(1) 对任何非零整数 a, $\gcd(a, 0) = |a|$.

(2) 对任何不全为零的整数 a 和 b, $\gcd(a, b) = \gcd(|a|, |b|)$.

证明　(1) 显然 $|a|$ 是 a 和 0 的公因子, 根据命题 1.1.1 (6) 知 $a, 0$ 的任何公因子 d 都满足 $d \leqslant \max\{|a|, 0\} = |a|$, 故 $|a| = \gcd(a, 0)$.

(2) 根据最大公因子的定义, 只需证明 a, b 和 a, $-b$ 有相同的公因子集, 而这显然是命题 1.1.1 (1) 的直接推论. □

1.2.2　辗转相除法

给定整数 a 和 b, 一个基本的问题是如何计算其最大公因子. 命题 1.2.1 表明只需考虑 a, b 为正整数的情形. 对于这个问题, 最直接的方法是分别列出 a 和 b 的所有正因子. 例如: $a = 30$, $b = -18$, 30 的正因子有 1, 2, 3, 5, 6, 10, 15, 30, -18 的正因子为 1, 2, 3, 6, 9, 18, 故 30 和 -18 的最大公因子为 6. 这种方法对于很大的正整数 a 和 b 来说是不切实际的, 其根本原因为整数因子分解之复杂性. 值得一提的是, 约公元前 300 年, Euclid 在《原本》中给出了一个非常有效的算法来计算两个正整数的最大公因子, 现被称为 **Euclid 算法**. 而在中国, 该方法则可追溯至《九章算术》中的**更相减损术**, 这个算法被南宋数学家秦九韶发展为解一次同余方程的**大衍求一术**, 因此又称为**辗转相除法**. 这个算法基于下面的引理.

引理1.2.1　设整数 a, b, q, r 满足

$$a = qb + r \quad \text{且} \quad b \neq 0,$$

则 $\gcd(a, b) = \gcd(b, r)$.

证明　由命题 1.1.1 (3) 知 b 和 r 的任一公因子都整除 $a = qb + r$. 类似地, a 和 b 的任一公因子都整除 $r = a - qb$. 因此 a, b 与 b, r 有相同的公因子集, 从而它们有相同的最大公因子. □

利用引理 1.2.1, 我们可将求两个正整数 a 和 b (不妨设 $a \geqslant b$) 的最大公因子转化为求 b 和 a 除以 b 所得余数 r 的最大公因子, 然后不断重复这个过程直到余数等于 0 为止, 那么最后的非零余数就是 a 和 b 的最大公因子. 具体操作如下.

由定理 1.1.1, 将 a 除以 b 的带余除法写为

$$a = q_1 b + r_1 \quad \text{且} \quad 0 \leqslant r_1 < b.$$

若 $r_1 = 0$, 由引理 1.2.1 知 $\gcd(a, b) = \gcd(b, r_1) = b$ 并停止操作. 否则 $r_1 > 0$, 再将 b 除以 r_1 的带余除法写为

$$b = q_2 r_1 + r_2 \quad \text{且} \quad 0 \leqslant r_2 < r_1,$$

同样有 $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2)$. 因此当 $r_2 = 0$ 时 $\gcd(a, b) = r_1$. 否则 $r_2 > 0$, 取整数 q_3, r_3 满足

$$r_1 = q_3 r_2 + r_3 \quad \text{且} \quad 0 \leqslant r_3 < r_2,$$

然后一直重复这种操作. 由于 $b > r_1 > r_2 > \cdots \geqslant 0$, 故经过有限 n 次带余除法后得到余数 $r_n = 0$, 必有 $n \leqslant b$. 最后两步为

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1} \quad \text{且} \quad 0 \leqslant r_{n-1} < r_{n-2};$$

$$r_{n-2} = q_n r_{n-1} + r_n \quad \text{且} \quad r_n = 0,$$

其中最后一个非零余数为 r_{n-1}. 由引理 1.2.1 知

$$\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) = r_{n-1}.$$

例1.2.1 计算 2024 和 1950 的最大公因子.

解 我们有

$$\begin{aligned} 2024 &= 1 \times 1950 + 74, \\ 1950 &= 26 \times 74 + 26, \\ 74 &= 2 \times 26 + 22, \\ 26 &= 1 \times 22 + 4, \\ 22 &= 5 \times 4 + 2, \\ 4 &= 2 \times 2 + 0. \end{aligned}$$

最后的非零余数为 2, 故 $\gcd(2024, 1950) = 2$.

注记 1.2.2 在进行辗转相除的过程中, 可将带余除法中关于余数 r_i 的条件 $0 \leqslant r_i < r_{i-1}$ 改为 $-\frac{r_{i-1}}{2} < r_i \leqslant \frac{r_{i-1}}{2}$. 这样我们只需不超过 $\log_2 b$ 次带余除法便可求出最大公因子. 详见习题 1, 2 和 3.

1.2.3　Bézout 定理

上一小节我们介绍了如何用辗转相除法求整数 a, b 的最大公因子. 现在我们来研究 a, b 和它们最大公因子的关系, 主要结果为如下定理:

定理 1.2.1(Bézout 定理)　*给定不全为零的整数 a 和 b. 则存在整数 u, v 使得*

$$\gcd(a,b) = ua + vb.$$

证明　不妨设 b 为正整数. 假设辗转相除的过程如下:

$$\begin{aligned}
a &= q_1 b + r_1 \quad \text{且} \quad 0 < r_1 < b;\\
b &= q_2 r_1 + r_2 \quad \text{且} \quad 0 < r_2 < r_1;\\
r_1 &= q_3 r_2 + r_3 \quad \text{且} \quad 0 < r_3 < r_2;\\
&\cdots\cdots\\
r_{n-4} &= q_{n-2} r_{n-3} + r_{n-2} \quad \text{且} \quad 0 < r_{n-2} < r_{n-3};\\
r_{n-3} &= q_{n-1} r_{n-2} + r_{n-1} \quad \text{且} \quad 0 < r_{n-1} < r_{n-2};\\
r_{n-2} &= q_n r_{n-1} + r_n \quad \text{且} \quad r_n = 0.
\end{aligned}$$

令 $d = \gcd(a,b)$. 根据倒数第二个方程的等价形式

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

d 可表为 r_{n-3} 与 r_{n-2} 的整数倍之和. 然后再结合倒数第三个方程的等价形式

$$r_{n-2} = r_{n-4} - q_{n-2} r_{n-3},$$

消去 r_{n-2} 知 d 可表为 r_{n-4} 与 r_{n-3} 的整数倍之和. 我们逐步逆推辗转相除过程中的方程并依次消去 $r_{n-3}, r_{n-4}, \cdots, r_1$, 最终可将 d 表为 a 与 b 的整数倍之和. 这就完成了定理的证明. □

推论1.2.1　*给定不全为零的整数 a 和 b.*

(1) *对任何整数 c, $c \mid a$ 且 $c \mid b$ 的充要条件为 $c \mid \gcd(a,b)$.*

(2) *考虑集合*

$$S = \{ua + vb \mid u, v \in \mathbb{Z}\},$$

则 $\gcd(a,b)$ 为集合 S 中的最小正整数.

(3) *对任何正整数 m, $\gcd(ma, mb) = m \cdot \gcd(a,b)$.*

(4) $\gcd\left(\dfrac{a}{\gcd(a,b)}, \dfrac{b}{\gcd(a,b)}\right) = 1.$

证明 (1) 充分性由最大公因子的定义可得. 对必要性, 假设 $c \mid a$ 且 $c \mid b$. 由 Bézout 定理知存在整数 u, v 使得 $\gcd(a,b) = ua + vb$, 再由命题 1.1.1 (3) 知 $c \mid \gcd(a,b)$.

(2) 由 Bézout 定理知 $\gcd(a,b) \in S$, 由命题 1.1.1 (3) 知 S 中任何正整数皆为 $\gcd(a,b)$ 的正整数倍, 从而 $\gcd(a,b)$ 为 S 中的最小正整数.

(3) 考虑集合

$$S' = \{u(ma) + v(mb) \mid u, v \in \mathbb{Z}\},$$

则 S' 中最小正整数等于 S 中最小正整数的 m 倍. 由 (2) 知 $\gcd(ma, mb) = m \cdot \gcd(a,b)$.

(4) 令 $d = \gcd(a,b)$. 由 (3) 有 $\gcd(a,b) = d \cdot \gcd\left(\dfrac{a}{d}, \dfrac{b}{d}\right)$, 故 $\gcd\left(\dfrac{a}{d}, \dfrac{b}{d}\right) = 1$. □

对给定不全为零的整数 $a_1, a_2, \cdots, a_k$, 其中 $k \geqslant 2$, 我们可类似地定义它们的最大公因子, 仍记为 $\gcd(a_1, a_2, \cdots, a_k)$. 对两个整数最大公因子的诸多性质大都适用于有限个整数的情形. 下面的引理可将对有限个整数的最大公因子之计算归结为两个整数的情形.

引理1.2.2 给定全不为零的整数 $a_1, a_2, \cdots, a_k$, 其中 $k \geqslant 2$. 我们有

$$\gcd(a_1, a_2, \cdots, a_k) = \gcd(\gcd(a_1, a_2), a_3, \cdots, a_k).$$

证明 令 $d = \gcd(a_1, a_2, \cdots, a_k)$, $e = \gcd(\gcd(a_1, a_2), a_3, \cdots, a_k)$. 我们有 $d \mid a_i$, $1 \leqslant i \leqslant k$. 由推论 1.2.1 (1) 知 $d \mid \gcd(a_1, a_2)$. 于是 d 是 $\gcd(a_1, a_2), a_3, \cdots, a_k$ 的公因子, 故 $d \leqslant e$.

另一方面, 由 $\gcd(a_1, a_2)$ 是 a_1, a_2 的公因子知, $\gcd(a_1, a_2), a_3, \cdots, a_k$ 的最大公因子 e 必为 $a_1, a_2, \cdots, a_k$ 的公因子, 从而 $e \leqslant d$. □

定理1.2.2(Bézout 定理的一般形式) 给定不全为零的整数 $a_1, a_2, \cdots, a_k$, 其中 $k \geqslant 2$. 则存在整数 $u_1, u_2, \cdots, u_k$ 使得

$$\gcd(a_1, a_2, \cdots, a_k) = u_1a_1 + u_2a_2 + \cdots + u_ka_k.$$

证明 本定理可直接由定理 1.2.1, 引理 1.2.2 和数学归纳法得到. 在此, 我们给一个不依赖于辗转相除法的证明. 令 d 为 S 中的最小正整数, 其中

$$S = \left\{ \sum_{i=1}^{k} u_i a_i \,\middle|\, u_i \in \mathbb{Z} \right\}.$$

我们只需证 $d = \gcd(a_1, a_2, \cdots, a_k)$. 取整数 u_i 使得 $d = \sum_{i=1}^{k} u_i a_i$. 根据定理 1.1.1, 存在整数 q 和 r 使得

$$a_1 = -qd + r \quad \text{且} \quad 0 \leqslant r < d.$$

则

$$r = a_1 + qd = (1 + qu_1)a_1 + \sum_{i=2}^{k}(qu_i)a_i \in S.$$

由 d 的最小性知 $r = 0$, 从而 $d \mid a_1$. 同理 d 整除每个 a_i, 即 d 为 $a_1, a_2, \cdots, a_k$ 的公因子, 故 $d \leqslant \gcd(a_1, a_2, \cdots, a_k)$. 另一方面, 由命题 1.1.1 (3) 知 $\gcd(a_1, a_2, \cdots, a_k) \mid d$. 这就证明了 $d = \gcd(a_1, a_2, \cdots, a_k)$. □

1.2.4　互素

定义1.2.3　设 $a_1, a_2, \cdots, a_k$ 是 k 个不全为零的整数. 若 $\gcd(a_1, a_2, \cdots, a_k) = 1$, 则称 $a_1, a_2, \cdots, a_k$ **互素**. 若对任何 $1 \leqslant i < j \leqslant k$, a_i 与 a_j 互素, 则称这 k 个整数**两两互素**.

定理1.2.3　给定 k 个不全为零的整数 $a_1, a_2, \cdots, a_k$, 其中 $k \geqslant 2$. 则 $a_1, a_2, \cdots, a_k$ 互素当且仅当存在整数 $u_1, u_2, \cdots, u_k$ 使得

$$1 = u_1a_1 + u_2a_2 + \cdots + u_ka_k.$$

证明　必要性为定理 1.2.2 的特殊情形. 对充分性, 设有整数 u_i 使得 $1 = \sum_{i=1}^{k} u_ia_i$. 令 $d = \gcd(a_1, a_2, \cdots, a_k)$. 由命题 1.1.1 (3) 知 d 整除 $\sum_{i=1}^{k} u_ia_i = 1$, 故 $d = 1$. □

Bézout 定理在处理最大公因子以及互素等相关问题极为有用, 我们以如下两个推论为例:

推论1.2.2　设 a, b, c 为整数且 a, b 不全为零, 令 $d = \gcd(a, b)$.

(1) 若 $a \mid c$ 且 $b \mid c$, 则 $\dfrac{ab}{d} \,\Big|\, c$. 特别地, 若 a 与 b 还互素, 则 $ab \mid c$.

(2) 若 $a \mid bc$, 则 $\dfrac{a}{d} \,\Big|\, c$. 特别地, 若 a 与 b 还互素, 则 $a \mid c$.

证明　由定理 1.2.1 知存在整数 u, v 满足 $d = ua + vb$.

(1) 设 $a \mid c$ 且 $b \mid c$, 于是存在整数 x 使得 $c = xa$, 从而 $b \mid xa$. 根据命题 1.1.1 (3) 得 b 整除 $uxa + vxb = xd$, 再由该命题 (5) 得 $\dfrac{a}{d}b$ 整除 $ax = c$. 特别地, 若 a 和 b 还互素, 则 $ab \mid c$.

(2) 设 $a \mid bc$. 根据命题 1.1.1 (3) 知 a 整除 $uac + vbc = dc$, 再由该命题中的 (5) 知 $\dfrac{a}{d} \,\Big|\, c$. 特别地, 若 a 和 b 还互素, 则 $a \mid c$. □

推论1.2.3　设 $a_1, a_2, \cdots, a_k$ 为 k 个整数, $a = a_1a_2 \cdots a_k$. 则整数 b 和 a 互素当且仅当 b 和每个 a_i 都互素.

证明 假设 b 和每个 a_i 都互素. 由定理 1.2.3 知对任何 $1 \leqslant i \leqslant k$, 存在整数 u_i 和 v_i 使 $u_i a_i + v_i b = 1$. 于是

$$1 = (u_1 a_1 + v_1 b)(u_2 a_2 + v_2 b) \cdots (u_k a_k + v_k b).$$

故存在 $u, v \in \mathbb{Z}$ 使得 $1 = ua + vb$. 再由定理 1.2.3 知 a 和 b 互素. 反之显然. □

1.2.5 最小公倍数

定义1.2.4 给定 k 个全不为零的整数 $a_1, a_2, \cdots, a_k$, 其中 $k \geqslant 2$.

(1) 如果整数 m 满足 $a_1 \mid m, a_2 \mid m, \cdots, a_k \mid m$, 则称 m 是这 k 个整数的**公倍数**.

(2) 这 k 个整数的**最小公倍数**定义为满足下列条件的唯一正整数 m:

(a) $a_1 \mid m, a_2 \mid m, \cdots, a_k \mid m$;

(b) 若正整数 c 满足 $a_1 \mid c, a_2 \mid c, \cdots, a_k \mid c$, 则 $m \leqslant c$.

我们用记号 $\operatorname{lcm}(a_1, a_2, \cdots, a_k)$ 表示 $a_1, a_2, \cdots, a_k$ 的最小公倍数.

最大公因子和最小公倍数的关系由下列定理给出:

定理1.2.4 设 a, b 为两个正整数. 则

$$ab = \operatorname{lcm}(a, b) \cdot \gcd(a, b).$$

证明 令 $d = \gcd(a, b)$. 则命题等价于 $\operatorname{lcm}(a, b) = \dfrac{ab}{d}$. 任取 a 和 b 的公倍数 c. 则由推论 1.2.2 (1) 知 $\dfrac{ab}{d} \Big| c$. 显然 $\dfrac{ab}{d}$ 是 a 和 b 的公倍数. 根据定义, $\operatorname{lcm}(a, b) = \dfrac{ab}{d}$. □

引理1.2.3 设 $a_1, a_2, \cdots, a_k$ 为 k 个正整数. 则 $a_1 a_2 \cdots a_k = \operatorname{lcm}(a_1, a_2, \cdots, a_k)$ 的充要条件为 $a_1, a_2, \cdots, a_k$ 两两互素.

证明 假设 $a_1, a_2, \cdots, a_k$ 两两互素. 对任何整数 c, 根据推论 1.2.2 (1), $a_1 \mid c$, $a_2 \mid c, \cdots, a_k \mid c$ 当且仅当 $a_1 a_2 \cdots a_k \mid c$. 由最小公倍数的定义知 $a_1 a_2 \cdots a_k = \operatorname{lcm}(a_1, a_2, \cdots, a_k)$.

反之, 假设 $a_1, a_2, \cdots, a_k$ 不两两互素. 不妨设 $d := \gcd(a_1, a_2) > 1$. 从而 $\dfrac{a_1 a_2 \cdots a_k}{d}$ 为 $a_1, a_2, \cdots, a_k$ 的公倍数, 因此 $a_1 a_2 \cdots a_k > \operatorname{lcm}(a_1, a_2, \cdots, a_k)$. □

引理1.2.4 设 $a_1, a_2, \cdots, a_k$ 为 k 个非零整数. 令 $a = \operatorname{lcm}(a_1, a_2, \cdots, a_k)$.

(1) 若 c 是 $a_1, a_2, \cdots, a_k$ 的公倍数, 则 $a \mid c$.

(2) 整数 $\dfrac{a}{a_1}, \dfrac{a}{a_2}, \cdots, \dfrac{a}{a_k}$ 互素.

证明 (1) 根据定理 1.1.1, 存在整数 q 和 r 使得 $c = qa + r$ 且 $0 \leqslant r < a$. 若 c 是 $a_1, a_2, \cdots, a_k$ 的公倍数, 则 $r = c - qa$ 也为 $a_1, a_2, \cdots, a_k$ 的公倍数. 根据最小公倍数的

定义知 $r=0$, 即 $a \mid c$.

(2) 令 d 为 $\dfrac{a}{a_1}, \dfrac{a}{a_2}, \cdots, \dfrac{a}{a_k}$ 的最大公因子. 则对任何 $1 \leqslant i \leqslant k$, 都有 $d \Big| \dfrac{a}{a_i}$, 即 $a_i \Big| \dfrac{a}{d}$. 从而 $\dfrac{a}{d}$ 为 $a_1, a_2, \cdots, a_k$ 的公倍数. 由 (1) 知 $a \Big| \dfrac{a}{d}$, 从而 $d=1$. □

1.3　一次不定方程

所谓 n **元一次不定方程**, 是指可以写成如下形式的方程

$$a_1x_1 + a_2x_2 + \cdots + a_nx_n = c, \tag{1.1}$$

其中 n 为正整数, $a_1, a_2, \cdots, a_n$ 为不全为零的整数, c 为整数, $x_1, x_2, \cdots, x_n$ 为不定元. 作为 Bézout 定理的应用, 我们有如下 n 元一次不定方程解的存在性定理.

定理 1.3.1　*不定方程 (1.1) 有整数解的充要条件为* $\gcd(a_1, a_2, \cdots, a_n) \mid c$.

证明　令 $d = \gcd(a_1, a_2, \cdots, a_n)$. 假设存在 n 个整数 $x_{10}, x_{20}, \cdots, x_{n0}$ 满足

$$a_1x_{10} + a_2x_{20} + \cdots + a_nx_{n0} = c.$$

由命题 1.1.1 (3) 知 d 整除 $a_1x_{10} + a_2x_{20} + \cdots + a_nx_{n0} = c$. 这就证明了必要性.

反之, 假设 $d \mid c$, 即 $\dfrac{c}{d}$ 为整数. 由定理 1.2.2 知存在整数 $u_1, u_2, \cdots, u_n$ 使得

$$a_1u_1 + a_2u_2 + \cdots + a_nu_n = d.$$

于是 $x_1 = \dfrac{c}{d}u_1, x_2 = \dfrac{c}{d}u_2, \cdots, x_n = \dfrac{c}{d}u_n$ 是 (1.1) 的整数解, 充分性得证. □

例1.3.1　设 a, c 为整数且 $a \neq 0$. 则不定方程

$$ax = c$$

有整数解当且仅当 $a \mid c$. 若其有整数解, 则解必为 $x = \dfrac{c}{a}$.

定理 1.3.2　*设* a, b, c *为整数, 其中* a, b *不全为零. 令* $d = \gcd(a, b)$. *则不定方程*

$$ax + by = c \tag{1.2}$$

有解当且仅当 $d \mid c$. *若* $x = x_0$, $y = y_0$ *为* (1.2) *的一组整数解, 则* (1.2) *的所有整数解为*

$$x = x_0 + \frac{bt}{d}, \quad y = y_0 - \frac{at}{d}, \tag{1.3}$$

其中 t *为任意整数.*

证明 解的存在性为定理 1.3.1 的特殊情形. 设 $x = x_0$, $y = y_0$ 为 (1.2) 的一组整数解, 即 $ax_0 + by_0 = c$. 对任何整数 t, 我们有

$$a\left(x_0 + \frac{bt}{d}\right) + b\left(y_0 - \frac{at}{d}\right) = ax_0 + by_0 = c,$$

即 $x = x_0 + \dfrac{bt}{d}$, $y = y_0 - \dfrac{at}{d}$ 也为 (1.2) 的整数解.

反之, 设整数 x_0', y_0' 满足 $ax_0' + by_0' = c$. 将其减去 $ax_0 + by_0 = c$, 可得

$$a(x_0' - x_0) = b(y_0 - y_0'). \tag{1.4}$$

因此 $a \mid b(y_0 - y_0')$. 根据推论 1.2.2 (2) 知 $\dfrac{a}{d} \mid y_0 - y_0'$, 即存在整数 t 使得 $y_0' = y_0 - \dfrac{at}{d}$. 代入 (1.4) 得 $x_0' = x_0 + \dfrac{bt}{d}$, 即 $x = x_0', y = y_0'$ 具有形式 (1.3). □

例1.3.2 求下列不定方程的所有整数解:

$$2024x + 1950y = 10. \tag{1.5}$$

解 由例 1.2.1 知 $\gcd(2024, 1950) = 2$. 从该例计算中的倒数第二个方程开始倒推可得

$$\begin{aligned}
2 &= 22 - 5 \times 4 \\
&= 22 - 5(26 - 22) \\
&= (-5) \times 26 + 6 \times 22 \\
&= (-5) \times 26 + 6(74 - 2 \times 26) \\
&= 6 \times 74 - 17 \times 26 \\
&= 6 \times 74 - 17(1950 - 26 \times 74) \\
&= (-17) \times 1950 + 448 \times 74 \\
&= (-17) \times 1950 + 448(2024 - 1950) \\
&= 448 \times 2024 + (-465) \times 1950,
\end{aligned}$$

因此 $x = 448$, $y = -465$ 满足方程 $2024x + 1950y = 2$. 从而 $x = 2240, y = -2325$ 为方程 (1.5) 的一组整数解. 根据定理 1.3.2, 方程 (1.5) 的所有整数解为

$$x = 2240 + 975t,\ y = -2325 - 1012t\ \ (t \in \mathbb{Z}).$$

例1.3.3 求下列不定方程的所有整数解:

$$6x + 10y + 15z = 1.$$

解 由定理 1.3.1 以及 $\gcd(6, 10, 15) = 1$ 知本方程有整数解. 由 $\gcd(10, 15) = 5$ 知求解本方程等价于求解方程组

$$\begin{cases} 6x+5w=1, \\ 2y+3z=w. \end{cases}$$

由于 $x=1, w=-1$ 是二元一次方程 $6x+5w=1$ 的一组整数解, 故此方程的所有整数解为

$$x=1+5t,\ w=-1-6t\ \ (t\in\mathbb{Z}). \tag{1.6}$$

将 w 看作常数, $y=-w,\ z=w$ 是二元一次方程 $2y+3z=w$ 的一组整数解, 则此方程所有的整数解为

$$y=-w+3s,\ z=w-2s\ \ (s\in\mathbb{Z}). \tag{1.7}$$

联立 (1.6) 和 (1.7) 并消去 w, 于是原方程的所有整数解为

$$x=1+5t,\ y=1+6t+3s,\ z=-1-6t-2s\quad (s,t\in\mathbb{Z}).$$

1.4　素数

这一节讨论素数的基本性质, 包括整数的素因子分解以及素数的判定与分布等问题, 其最重要的结果为算术基本定理以及 Chebyshev 不等式.

1.4.1　素数的基本性质

对任何大于 1 的整数 a, 1 和 a 都是 a 的正因子, 我们称这两个因子为平凡正因子. 据此, 我们可把大于 1 的正整数分为如下两类:

定义1.4.1　一个大于 1 的整数, 如果它的正因子只有 1 和自身, 则称之为**素数**, 否则称之为**合数**.

例如,

$$2,3,5,7,11,13,17,19,23,29,31,37,41,43,47$$

为小于 50 的所有素数. 由合数的定义不难看出: 正整数 a 为合数当且仅当 a 可写为两个小于 a 的正整数之积.

定理1.4.1　设 p 为大于 1 的整数, 下列三个条件等价:

(1) p 是素数.

(2) 对任何整数 a, 要么 $p\mid a$, 要么 p 与 a 互素.

(3) 对任何整数 a 和 b, 若 $p \mid ab$, 则 $p \mid a$ 或 $p \mid b$.

证明 设 p 为素数. 对任何整数 a, $\gcd(a,p)$ 为 p 的正因子, 从而 $\gcd(a,p)=1$ 或者 $\gcd(a,p)=p$. 当 $\gcd(a,p)=1$ 时, a 和 p 互素, 而当 $\gcd(a,p)=p$ 时, $p \mid a$. 这就证明了 (1) $\Longrightarrow$ (2).

假设 (2) 成立. 任给整数 a,b 满足 $p \mid ab$. 若 $p \nmid a$, 根据假设 p 和 a 互素. 从而由推论 1.2.2 (2) 得 $p \mid b$. 这就证明了 (2) $\Longrightarrow$ (3).

若 p 不是素数, 则存在两个小于 p 的正整数 a, b 使得 $p=ab$. 此时, $p \nmid a$ 且 $p \nmid b$. 这就证明了 (3) $\Longrightarrow$ (1). □

推论1.4.1 设 p 为素数, $a_1,a_2,\cdots,a_k$ 为 k 个整数. 若 $p \mid a_1a_2\cdots a_k$, 则 p 整除某个 a_i.

定理1.4.2 对任何大于 1 的整数 a, 必存在素数 p 使得 $p \mid a$.

证明 令 S 为 a 所有大于 1 的因子组成的集合. 由假设 $a>1$ 知 $a \in S$. 根据最小自然数原理, S 中必有最小的整数, 记为 p. 若 p 是合数, 则存在小于 p 的正整数 x 和 y 满足 $p=xy$, 故 $x>1$. 由 $x \mid p$ 和 $p \mid a$ 知 $x \mid a$, 即 $x \in S$, 这和 p 是 S 中的最小整数矛盾. 故 p 是素数. □

1.4.2 算术基本定理

如果一个整数的因子是素数, 则称该因子为**素因子**. 这一章的主要结果为如下的定理:

定理1.4.3(算术基本定理) 任一大于 1 的整数均可分解为有限个素数的乘积, 若不考虑顺序的话, 这种表达方式是唯一的. 准确地说, 设 n 为大于 1 的整数, 则 n 可写为

$$n=p_1p_2\cdots p_r,$$

其中 $p_1,p_2,\cdots,p_r$ 为素数且 $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_r$. 若 n 还可写为

$$n=q_1q_2\cdots q_s,$$

其中 $q_1,q_2,\cdots,q_s$ 为素数且 $q_1 \leqslant q_2 \leqslant \cdots \leqslant q_s$, 则 $r=s$ 且对任何 $1 \leqslant i \leqslant r$ 都有 $p_i=q_i$.

证明 先用第二数学归纳法证明分解的存在性. 当 $n=2$ 时, 2 为素数, 结论显然成立. 假设整数 $k>2$, 并且当 $2 \leqslant n<k$ 时, 结论对 n 成立. 若 k 是素数, 则结论对 $n=k$ 显然成立. 否则 k 为合数, 于是 k 可写为两个小于 k 的正整数 k_1 和 k_2 之积. 由归纳假设知 k_1,k_2 均可写为素数的乘积:

$$k_1=p_{11}p_{12}\cdots p_{1r_1},\ k_2=p_{21}p_{22}\cdots p_{2r_2}.$$

于是 k 可写为素数的乘积

$$k = p_{11}p_{12}\cdots p_{1r_1}p_{21}p_{22}\cdots p_{2r_2}.$$

这就完成了对分解存在性的归纳证明.

现在来证明分解的唯一性. 假设

$$n = p_1p_2\cdots p_r = q_1q_2\cdots q_s, \tag{1.8}$$

其中 $p_1, p_2, \cdots, p_r, q_1, q_2, \cdots, q_s$ 为素数且 $p_1 \leqslant p_2 \leqslant \cdots \leqslant p_r$, $q_1 \leqslant q_2 \leqslant \cdots \leqslant q_s$. 故 $p_1 \mid q_1q_2\cdots q_s$. 由推论 1.4.1 知存在 $1 \leqslant j \leqslant s$ 使得 $p_1 \mid q_j$. 由于 p_1 与 q_j 皆为素数, 必有 $p_1 = q_j$, 因此 $p_1 = q_j \geqslant q_1$. 同理, $q_1 \geqslant p_1$, 故而 $p_1 = q_1$. 代入 (1.8) 得

$$p_2p_3\cdots p_r = q_2q_3\cdots q_s,$$

同理可得 $p_2 = q_2$. 依次类推, 最后可得 $r = s$, $p_1 = q_1, p_2 = q_2, \cdots, p_r = q_r$. □

由算术基本定理马上可以得出

推论1.4.2　*任一大于 1 的整数 n 可以唯一地写成*

$$n = p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}, \tag{1.9}$$

其中 $p_1, p_2, \cdots, p_r$ 为素数且 $p_1 < p_2 < \cdots < p_r$, $\alpha_1, \alpha_2, \cdots, \alpha_r$ 为正整数.

(1.9) *称为 n 的***标准分解式**.

由 $720 = 2\times2\times2\times2\times3\times3\times5$ 知 720 的标准分解式为 $720 = 2^4\times3^2\times5$. 标准分解式在计算两个正整数的积、商、最大公因子、最小公倍数以及判定它们的整除关系时非常方便. 我们有下列简单命题:

命题1.4.1　*设*

$$a = \prod_{i=1}^{r} p_i^{\alpha_i},\ b = \prod_{i=1}^{r} p_i^{\beta_i},$$

其中 $p_1, p_2, \cdots, p_r$ 为两两不同的素数, 所有 α_i, β_i 为自然数. 则

$$ab = \prod_{i=1}^{r} p_i^{\alpha_i+\beta_i};$$

$$\frac{a}{b} = \prod_{i=1}^{r} p_i^{\alpha_i-\beta_i};$$

$$a^k = \prod_{i=1}^{r} p_i^{k\alpha_i};$$

$$\gcd(a,b) = \prod_{i=1}^{r} p_i^{\min\{\alpha_i,\beta_i\}};$$

$$\operatorname{lcm}(a,b)=\prod_{i=1}^{r}p_i^{\max\{\alpha_i,\beta_i\}};$$

$$a\mid b\Leftrightarrow \alpha_i\leqslant\beta_i,\ 1\leqslant i\leqslant r.$$

定义1.4.2 设 p 是素数, a 是非零整数, d 为自然数. 若 $p^d\mid a$ 但 $p^{d+1}\nmid a$, 则称 p^d **恰好整除** a, d 为素数 p 在 a 中的**指数**. 我们用记号 $p^d\parallel a$ 表示 p^d 恰好整除 a, 用 $v_p(a)$ 表示 p 在 a 中的指数.

命题1.4.2 令 $\mathbb{P}$ 为所有素数组成的集合. 我们有如下简单性质:

(1) 对任何非零整数 a, 我们有

$$a=\operatorname{sgn}(a)\prod_{\mathbb{P}\ni p}p^{v_p(a)}=\operatorname{sgn}(a)\prod_{\mathbb{P}\ni p\mid a}p^{v_p(a)}.$$

(2) 对素数 p 和非零整数 a, $p^0\parallel a\iff v_p(a)=0\iff p\nmid a$.

(3) 对素数 p 和非零整数 a 和 b, 我们有 $v_p(ab)=v_p(a)+v_p(b)$.

命题1.4.3 设 p 为素数. 则对任何正整数 n, 我们有

$$v_p(n!)=\sum_{i=1}^{+\infty}\left\lfloor\frac{n}{p^i}\right\rfloor.$$

证明 我们有

$$v_p(n!)=\sum_{k=1}^{n}v_p(k)=\sum_{k=1}^{n}\sum_{\substack{i\geqslant 1\\ p^i\mid k}}1=\sum_{i=1}^{+\infty}\sum_{\substack{1\leqslant k\leqslant n\\ p^i\mid k}}1=\sum_{i=1}^{+\infty}\left\lfloor\frac{n}{p^i}\right\rfloor.\qquad\square$$

定义1.4.3 设 k 为正整数. 如果一个整数可以写成某个整数的 k 次方, 则称该整数为 k **次方数**. 对于 2 次方数, 我们也称之为**完全平方数**. 按照定义, 0 和 1 都是 k 次方数.

命题1.4.4 设 $a_1,a_2,\cdots,a_r$ 为两两互素的正整数, $k\geqslant 2$ 为整数. 则 $a_1a_2\cdots a_r$ 为 k 次方数当且仅当每个 a_i 皆为 k 次方数.

证明 首先由正整数 n 的标准分解式知, n 是 k 次方数的充要条件为对任何素数 p 都有 $k\mid v_p(n)$. 令 $a=a_1a_2\cdots a_r$.

假设每个 a_i 为 k 次方数, 即 $k\mid v_p(a_i)$. 根据命题 1.4.2 (3), k 整除 $v_p(a)=\sum_{i=1}^{r}v_p(a_i)$. 故 a 为 k 次方数.

反之, 假设 a 为 k 次方数. 要证 a_i 为 k 次方数, 只需证对 a_i 的任何素因子 p, 都有 $k\mid v_p(a_i)$. 由于 $a_1,a_2,\cdots,a_r$ 两两互素, 因此当 $j\neq i$ 时, 我们有 $v_p(a_j)=0$. 故 $v_p(a_i)=\sum_{j=1}^{r}v_p(a_j)=v_p(a)$. 由假设 a 为 k 次方数知 $k\mid v_p(a)$, 于是 $k\mid v_p(a_i)$. $\square$

推论1.4.3　设大于 1 的正整数 a 不是 k 次方数, 其中 $k \geqslant 1$. 则 $\sqrt[k]{a}$ 为无理数.

证明　用反证法. 假设 $\sqrt[k]{a}$ 为有理数, 则存在正整数 b, c 使得 $\sqrt[k]{a} = \dfrac{b}{c}$. 于是 $a = \dfrac{b^k}{c^k}$. 任取 a 的素因子 p. 根据命题 1.4.2 (3), 我们有 $v_p(a) = kv_p(b) - kv_p(c)$. 因此 $k \mid v_p(a)$, 从而 a 为 k 次方数, 这与假设矛盾. 故 $\sqrt[k]{a}$ 为无理数. □

1.4.3　Eratosthenes 筛法

关于判定给定整数是否为素数的问题, 我们有如下引理:

引理1.4.1　一个大于 1 的整数 n 为合数当且仅当 n 有素因子 $p \leqslant \sqrt{n}$.

证明　假设 n 有素因子 $p \leqslant \sqrt{n}$, 则 $n = p \cdot \dfrac{n}{p}$, 其中整数 $\dfrac{n}{p} \geqslant \sqrt{n} > 1$, 从而 n 为合数.

反之, 假设 n 为合数. 记其最小素因子为 q, 则 $\dfrac{n}{q}$ 为大于 1 的整数且其所有素因子均不小于 q, 于是 $\dfrac{n}{q} \geqslant q$, 从而 $q \leqslant \sqrt{n}$. □

例如, 131 为素数, 这是因为不超过 $\sqrt{131}$ 的素数只有 $2, 3, 5, 7, 11$, 而 131 不能被这 5 个素数中的任何一个整除. 实际上, 引理 1.4.1 也给出了寻找素数的一种方法. 例如, 若要求出不超过给定正整数 n 的所有素数, 只需把 1 和不超过 n 的所有合数去掉. 由引理 1.4.1 知不超过 n 的合数必有不超过 $\sqrt{n}$ 的素因子, 因此只要先求出不超过 $\sqrt{n}$ 的所有素数, 然后在大于 1 且不超过 n 的这些整数中删去这些素数除本身之外的倍数, 那么剩下的数恰为不超过 n 的所有素数. 这种方法被称为 **Eratosthenes 筛法**. 具体做法详见图 1.1, 其中 n 取 100.

	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~~

图 1.1

注意到不超过 $\sqrt{n} = 10$ 的素数只有 $2, 3, 5, 7$. 首先划去除 2 之外所有 2 的倍数, 用记号 ~~4~~, ~~6~~ 等表示, 然后划去除 3 之外所有 3 的倍数, 用记号 ~~9~~, ~~15~~ 等表示, 接着划去除 5 之外所有 5 的倍数, 用记号 ~~25~~, ~~35~~ 等表示, 最后划去除 7 之外所有 7 的倍数, 用 ~~49~~, ~~77~~

等表示. 于是图 1.1 中剩下的数则为所有不超过 100 的素数, 分别为

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

1.4.4 素数分布

研究素数的性质是数论的核心问题之一, 至今对这一问题了解不是很多. 这一小节我们对素数的个数做初步的讨论. 我们有如下定义:

定义1.4.4 将全体素数从小至大排列, 记 p_n 为第 n 个素数. 对任何正实数 x, 令 $\pi(x)$ 为不大于 x 的素数个数.

第一个关于素数分布的结果可以追溯到公元前 300 年左右的 Euclid.

定理1.4.4(Euclid) 素数有无穷多个.

证明 反证法. 假设只有有限个素数, 它们为 $p_1,p_2,\cdots,p_r$. 令 $n=p_1p_2\cdots p_r+1$. 由定理 1.4.2 知 n 存在素因子 p. 根据假设, p 等于某个 p_i, 从而 p_i 整除 $n-p_1p_2\cdots p_r=1$, 这与 p_i 为素数矛盾. 故存在无穷个素数. □

用证明定理 1.4.4 同样的方法我们可以得出正整数的一些特殊子集中依然包含无限个素数.

定理1.4.5 存在无穷个形如 $4k+3$ 的素数, 其中 k 为自然数.

证明 假设只有有限个形如 $4k+3$ 的素数 $p_1,p_2,\cdots,p_r$. 令 $n=4p_1p_2\cdots p_r-1$, 故 n 也形如 $4k+3$. 因 n 为奇数, 则 n 的任何素因子 p 也为奇数, 故 p 形如 $4k+1$ 或 $4k+3$. 若 n 的所有素因子都形如 $4k+1$, 由于 n 为其素因子的乘积, 从而 n 必形如 $4k+1$. 这和 n 形如 $4k+3$ 矛盾, 故 n 必有形如 $4k+3$ 的素因子 p. 由假设知存在 $1\leqslant i\leqslant r$ 使得 $p=p_i$, 故 $p_i\mid n$. 于是 p_i 整除 $4p_1p_2\cdots p_r-n=1$, 这与 p_i 是素数矛盾, 故命题得证. □

实际上, 形如 $4k+1$ 的素数也有无穷多个, 但其证明要比 $4k+3$ 的情形困难很多, 其具体证明将在定理 5.2.2 中给出. 更一般地, Dirichlet 将上述结果推广到算术级数上:

定理1.4.6(Dirichlet, 1837) 设 a,b 为互素的正整数, 则存在无限个形如 $ak+b$ 的素数, 其中 k 为正整数.

Dirichlet 为了证明他的定理, 推广了当时刚出现不久的 Fourier 分析到有限 Abel 群上去, 引入了特征理论和 Dirichlet L-函数, 这标志着解析数论这门学科的正式开始. 本书并不给出这个定理的证明, 感兴趣的读者可以参考诸多解析数论的书籍, 例如 [Dav2].

根据定理 1.4.4 的证明, 下面我们给出不超过 x 的素数个数 $\pi(x)$ 的一个很弱的下界以及第 n 个素数 p_n 的一个很弱的上界.

推论1.4.4 (1) 对任何正整数 n, $p_n\leqslant 2^{2^{n-1}}$.

(2) 对任何实数 $x\geqslant 2$, $\pi(x)>\log_2(\log_2 x)$.

证明　(1) 对 n 用第二数学归纳法. 当 $n=1$ 时, $p_1=2=2^{2^0}$. 假设命题对 $n\leqslant k$ 都成立, 其中 $k\geqslant 1$. 当 $n=k+1$ 时, 由定理 1.4.4 的证明知 $p_1p_2\cdots p_k+1$ 必有不等于 $p_1,p_2,\cdots,p_k$ 的素因子 p. 于是

$$p_{k+1}\leqslant p\leqslant p_1p_2\cdots p_k+1\leqslant 2^1\cdot 2^2\cdots 2^{2^{k-1}}+1=2^{1+2+\cdots+2^{k-1}}+1=2^{2^k-1}+1\leqslant 2^{2^k}.$$

这就完成了 (1) 的归纳证明.

(2) 根据 $\pi(x)$ 的定义, $p_{\pi(x)}\leqslant x<p_{\pi(x)+1}$. 由 (1) 知 $x<p_{\pi(x)+1}\leqslant 2^{2^{\pi(x)}}$, 即 $\pi(x)>\log_2(\log_2 x)$. □

注记1.4.1　推论 1.4.4 中的估计非常弱. 事实上, $\pi(x)$ 要远远大于 $\log_2(\log_2 x)$. Legendre 和 Gauss 在 1800 年左右独立提出了 $\pi(x)$ 的渐近公式:

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

其中 $\ln x=\log_{\mathrm{e}} x$ 为自然对数. 这个猜测直到 1896 年才被 Hadamard 与 de la Vallée Poussin, 利用高深的复变函数理论独立证明. 而它的初等证明, 则要到 1949 年才由 Selberg 与 Erdös 独立给出, 但是十分复杂. 这些都超出本书的范围, 本章最后用初等方法给出 $\pi(x)$ 的上界和下界估计, 即 Chebyshev 不等式.

定理1.4.7(Chebyshev)　对任何实数 $x\geqslant 2$ 和正整数 $n\geqslant 2$, 我们有

$$\frac{\ln 2}{3}\frac{x}{\ln x}<\pi(x)<6\ln 2\frac{x}{\ln x},\tag{1.10}$$

$$\frac{1}{6\ln 2}n\ln n<p_n<\frac{8}{\ln 2}n\ln n.\tag{1.11}$$

证明　对正整数 m, 令 $M=\dfrac{(2m)!}{(m!)^2}$. 根据推论 1.4.2, 我们有

$$\begin{aligned}\ln M&=\ln((2m)!)-2\ln(m!)\\&=\sum_{p\leqslant 2m}(v_p((2m)!)-2v_p(m!))\ln p\\&=\sum_{p\leqslant m}(v_p((2m)!)-2v_p(m!))\ln p+\sum_{m<p\leqslant 2m}(v_p((2m)!)-2v_p(m!))\ln p,\end{aligned}\tag{1.12}$$

其中求和号中的 p 特指素数. 显然我们有

$$v_p((2m)!)-2v_p(m!)=1\quad(m<p\leqslant 2m).\tag{1.13}$$

注意到对任何实数 y, 我们有 $0\leqslant\lfloor 2y\rfloor-2\lfloor y\rfloor\leqslant 1$. 从而根据命题 1.4.3, 我们有

$$0 \leqslant v_p((2m)!) - 2v_p(m!) = \sum_{i=1}^{+\infty} \left(\left\lfloor \frac{2m}{p^i} \right\rfloor - 2\left\lfloor \frac{m}{p^i} \right\rfloor \right) \leqslant \left\lfloor \frac{\ln(2m)}{\ln p} \right\rfloor \leqslant \frac{\ln(2m)}{\ln p}. \tag{1.14}$$

综合 (1.12), (1.13) 和 (1.14) 得

$$\sum_{m<p\leqslant 2m} \ln p \leqslant \ln M \leqslant \sum_{p\leqslant 2m} \ln(2m).$$

因此

$$(\pi(2m) - \pi(m)) \ln m \leqslant \ln M \leqslant \pi(2m) \ln(2m). \tag{1.15}$$

另一方面, 我们有

$$\begin{aligned} M = \prod_{i=1}^{m} \frac{m+i}{i} &\geqslant \prod_{i=1}^{m} 2 = 2^m, \\ M &< (1+1)^{2m} = 2^{2m}. \end{aligned} \tag{1.16}$$

由 (1.15) 和 (1.16) 可得

$$\pi(2m) \ln(2m) \geqslant m \ln 2, \tag{1.17}$$

$$(\pi(2m) - \pi(m)) \ln m < 2m \ln 2. \tag{1.18}$$

当 $x \geqslant 6$ 时, 在 (1.17) 中令 $m = \left\lfloor \frac{x}{2} \right\rfloor$, 我们有 $3m > x \geqslant 2m$, 并且

$$\pi(x) \ln x > \frac{\ln 2}{3} x.$$

通过直接验证可知上式对 $2 \leqslant x \leqslant 6$ 依然成立, 这就证明了 (1.10) 的左半不等式.

在 (1.18) 中令 $m = 2^k$, 我们有

$$k\pi(2^{k+1}) - k\pi(2^k) \leqslant 2^{k+1},$$

其中 k 为自然数. 显然有 $\pi(2^{k+1}) \leqslant 2^k$, 从而

$$(k+1)\pi(2^{k+1}) - k\pi(2^k) \leqslant 3 \cdot 2^k.$$

因此

$$(m+1)\pi(2^{m+1}) = \sum_{k=0}^{m} \left((k+1)\pi(2^{k+1}) - k\pi(2^k) \right) \leqslant 3 \sum_{k=0}^{m} 2^k < 3 \cdot 2^{m+1}.$$

对任何实数 $x \geqslant 2$, 存在唯一正整数 l 使得 $2^l \leqslant x < 2^{l+1}$. 于是

$$\pi(x) \leqslant \pi(2^{l+1}) < \frac{3 \cdot 2^{l+1}}{l+1} \leqslant 6 \ln 2 \frac{x}{\ln x}.$$

即 (1.10) 的右半不等式成立.

在 (1.10) 中取 $x = p_n$, 并利用 $p_n > n$ 可得

$$n < 6\ln 2\frac{p_n}{\ln p_n} < 6\ln 2\frac{p_n}{\ln n},$$

即 (1.11) 的左半不等式成立. 对任何整数 $n \geqslant 2$, 在 (1.17) 中令 $m = \dfrac{p_n+1}{2}$, 我们有

$$n\ln(p_n+1) \geqslant \frac{\ln 2}{2}(p_n+1). \tag{1.19}$$

于是

$$\ln n + \ln\ln(p_n+1) \geqslant \ln(p_n+1) + \ln\ln 2 - \ln 2. \tag{1.20}$$

对任何实数 $t \geqslant 0$, 我们有

$$\mathrm{e}^t - 2t = \sum_{i=0}^{+\infty}\frac{t^i}{i!} - 2t \geqslant 1 - t + \frac{t^2}{2} = \left(1-\frac{t}{2}\right)^2 + \frac{1}{4}t^2 > 0.$$

上式对 $t < 0$ 显然成立, 故上式对任何实数 t 皆成立. 特别地, 取 $t = \ln\ln(p_n+1)$, 有

$$\ln\ln(p_n+1) < \frac{\ln(p_n+1)}{2}.$$

将上式代入 (1.20) 得

$$\ln(p_n+1) < 2\ln n + 2(\ln 2 - \ln\ln 2).$$

由于 $\dfrac{2}{\ln 2} < 3$, 从而当 $n \geqslant 3$ 时我们有

$$\ln(p_n+1) < 4\ln n.$$

将上式代入 (1.19) 可得当 $n \geqslant 3$ 时, (1.11) 的右半不等式成立, 而当 $n = 2$ 时直接验证可得 (1.11) 的右半不等式成立. □

习题

1. 设 a, b 是两个整数, 其中 $b \neq 0$. 证明: 存在唯一的一对整数 q 和 r, 使得

$$a = qb + r \quad \text{且} \quad -\left|\frac{b}{2}\right| < r \leqslant \left|\frac{b}{2}\right|.$$

这种带余除法被称为**最小带余除法**.

2. 利用最小带余除法计算 $\gcd(2024, 1950)$.

3. 设 a, b 是两个正整数. 证明: 只需进行不超过 $\log_2(\min\{a,b\})$ 次最小带余除法便

可算出 a, b 的最大公因子.

4. 任一有理数均可唯一地写为分数 $\dfrac{p}{q}$, 其中 p, q 为互素的整数并且 $q>0$. 我们把这种形式的分数称为**既约分数**.

5. (1) 用辗转相除法计算 9797 和 155006 的最大公因子 d.

(2) 求下列不定方程的所有整数解:

$$9797x+155006y=d.$$

6. 设 a, b 为互素的正整数, n 为整数. 证明: 存在唯一的整数 u 和 v, 使得

$$n=ua+vb \quad \text{且} \quad 0\leqslant v<a.$$

7. 设 a 和 b 为互素的正整数.

(1) 证明: 任何大于 $ab-a-b$ 的整数均可写为 $ua+vb$, 其中 $u,v\in\mathbb{N}$.

(2) 证明: $ab-a-b$ 不能写成上述形式.

(3) 求不能写成上述形式的正整数个数.

8. 给定整数 $a\geqslant 2$. 证明: 任何正整数 n 可唯一地写为

$$n=\sum_{i=0}^{k} r_i a^i,$$

其中整数 $k\geqslant 0$, $0\leqslant r_i\leqslant a-1$, $r_k\geqslant 1$. 我们称这个表达式为 n 的 a **进制**展开.

9. 找出所有的整数 n, 使得 $n+1$ 整除 n^2+1.

10. 对任何正整数 n, 证明: n^2 整除 $(n+1)^n-1$.

11. 对任何正整数 n, 证明: 2015^n-1 都不能被 1000^n-1 整除.

12. 若 p 是大于 1 的整数, 证明: 3^p+1 不能被 2^p 整除.

13. 设正整数 a,m,n 满足 $a>1$. 证明:

$$\gcd(a^m-1,a^n-1)=a^{\gcd(m,n)}-1.$$

14. 设非零整数 a, b, c 满足 $c\mid ab$. 证明: $c\mid \gcd(a,c)\cdot\gcd(b,c)$.

15. 设非零整数 a, b, c 中有两个互素. 证明:

$$\gcd(a,bc)=\gcd(a,b)\cdot\gcd(a,c).$$

16. 设 a, b, c, d 为四个整数. 证明下列条件等价:

(1) 对任何整数 k, $ak+b$ 与 $ck+d$ 互素.

(2) $|ad-bc|=1$.

17. 设整数 a,b,c,d 满足 $|ad-bc|=1$. 证明: 对任何整数 u,v 都有

$$\gcd(u,v)=\gcd(au+bv,cu+dv).$$

18. 设 a, b 为不同的两个整数. 证明: 存在无穷多个整数 n, 使得 $a+n$ 和 $b+n$ 互素.

19. 给定互素的整数 a 和 b. 证明: $a+b$ 和 a^2+b^2 的最大公因子是 1 或 2.

20. 设 $f(x)=x^2-x+1$. 证明: 对任何自然数 m,

$$f(m),\ \ f(f(m)),\ \ f(f(f(m))),\ \ \cdots$$

两两互素.

21. 求不定方程 $1=17x+76y$ 的所有整数解.

22. 将分子、分母为不超过 99 的正整数的所有分数从小到大排列. 求 $\dfrac{17}{76}$ 左边与右边相邻的两个分数.

23. (1) 设 n 为使 2^n+1 是素数的正整数. 证明: n 为 2 的幂. 我们称形如 2^n+1 的素数为 **Fermat 素数**.

(2) 对任何自然数 n, 考虑 **Fermat 数** $F_n=2^{2^n}+1$. 当 $n\neq m$ 时, 证明: F_n 与 F_m 互素, 并由此推出素数有无穷多个.

24. (1) 对任何正整数 n, 若 2^n-1 为素数, 则 n 也为素数.

(2) 将形如 2^p-1 的数称为 **Mersenne 数**, 其中 p 为素数. 证明: 任何两个不同的 Mersenne 数都互素.

25. 证明: 存在无穷多个形如 $6k-1$ 的素数, 其中 $k\in\mathbb{N}$.

26. 求满足条件 $p^2\mid q^3+1,\ q^2\mid p^6-1$ 的所有素数对 $p,\ q$.

27. 设 $p_1,p_2,\cdots,p_n$ 是 n 个大于 3 的两两不同的素数. 证明: $2^{p_1p_2\cdots p_n}+1$ 至少有 4^n 个正因子.

28. 证明: 存在无穷多个整数 n, 使得 n^2+1 的每个素因子都小于 n.

29. 求所有的素数 p, 使得 p^2+71 的正因子个数不超过 10.

30. 设正整数 n 使得 $3n+1$ 和 $10n+1$ 均为完全平方数. 证明: $29n+11$ 是合数.

31. 设正整数 a,b,c,d 满足 $a^2-ab+b^2=c^2-cd+d^2$. 证明: $a+b+c+d$ 是合数.

32. 对于任意正整数 n, 证明: $n^{n^{n^n}}+n^{n^n}+n^n-1$ 是合数.

33. 给定素数 p 和正整数 k. 证明: 对任何整数 $1\leqslant i\leqslant p^k-1$, 都有 $p\left|\dbinom{p^k}{i}\right.$.

34. 给定整数 $n\geqslant 2$, 计算下列组合数的最大公因子:

$$\binom{n}{1},\ \binom{n}{2},\ \cdots,\ \binom{n}{n-1}.$$

35. 给定素数 p 并约定 $v_p(0)=+\infty$. 对任何整数 a 和 b, 证明:

$$v_p(ab)=v_p(a)+v_p(b),$$

$$v_p(a\pm b)\geqslant\min\{v_p(a),v_p(b)\}.$$

36. 对任何素数 p 和有理数 α, 定义

$$v_p(\alpha) = v_p(a) - v_p(b),$$

其中 a, b 为满足 $\alpha = \dfrac{a}{b}$ 的整数. 证明:

(1) $v_p(\alpha)$ 的定义不依赖于整数 a, b 的选取, 并且满足和上题类似的性质.

(2) 有理数 α 为整数的充要条件为对任何素数 p, 都有 $v_p(\alpha) \geqslant 0$.

37. 设映射

$$v : \mathbb{Q} \to \mathbb{Z} \cup \{+\infty\}$$

为满射并且满足: 对任何有理数 a 和 b, 都有

$$v(0) = +\infty,$$

$$v(ab) = v(a) + v(b),$$

$$v(a \pm b) \geqslant \min\{v(a), v(b)\}.$$

证明: 存在唯一的素数 p 使得 $v = v_p$.

38. 设 $n_1, n_2, \cdots, n_r$ 为 $r \geqslant 1$ 个正整数, $n = \sum_{i=1}^{r} n_i$. 证明: $\dfrac{n!}{n_1! n_2! \cdots n_r!}$ 为整数.

39. 对任何正整数 n, 证明: $2^{2^n} - 1$ 至少有 n 个不同的素因子.

40. 证明: 正整数 n 为完全平方数当且仅当 n 的正因子个数为奇数.

41. 称正整数 n 为**完全数**, 是指 n 的全部正因子之和等于 $2n$. 证明: n 为偶完全数的充要条件为 n 形如 $2^{p-1}(2^p - 1)$, 其中 p 和 $2^p - 1$ 均为素数.