第一章　整除性

1. 整除
2. 最大公因数与欧几里得算法
3. 最小公倍数
4. 一次不定方程
5. 算术基本定理
6. 厄拉多塞筛法
7. 素数分布

$\mathbb{Z}^+$: **自然数**或者**正整数**指的是数 $1, 2, \ldots$.

$\mathbb{Z}$: **整数**指的是数 $0, \pm 1, \pm 2, \ldots$.

显然, 任意 $a, b \in \mathbb{Z}$, 有 $a+b, a-b, ab \in \mathbb{Z}$, 即 $\mathbb{Z}$ 关于加, 减, 乘是封闭的, 但存在 $a, b \in \mathbb{Z}$ 使得 $a/b \notin \mathbb{Z}$. 因此我们需要考虑整除, 即研究什么时候 $a/b \in \mathbb{Z}$.

$\mathbb{Z}^+$: **自然数**或者**正整数**指的是数 $1, 2, \ldots$.

$\mathbb{Z}$: **整数**指的是数 $0, \pm 1, \pm 2, \ldots$.

显然, 任意 $a, b \in \mathbb{Z}$, 有 $a+b, a-b, ab \in \mathbb{Z}$, 即 $\mathbb{Z}$ 关于加, 减, 乘是封闭的, 但存在 $a, b \in \mathbb{Z}$ 使得 $a/b \notin \mathbb{Z}$. 因此我们需要考虑整除, 即研究什么时候 $a/b \in \mathbb{Z}$.

定义 1.1. 设 $a, b \in \mathbb{Z}$, 且 $b \neq 0$. 如果存在 $q \in \mathbb{Z}$ 使得 $a = bq$, 则称 b **整除**a, 记作 $b|a$. 此时, b 叫做 a 的**因数**, a 叫做 b 的**倍数**.

如果 b 不能整除 a, 则用记号 $b \nmid a$ 表示.

对任意整数 a, 显然 $1|a$, 即 1 是任意整数的因数; 当 $a \neq 0$ 时有 $a|0$ 和 $a|a$

由整除的定义, 我们不难证明下面这些基本性质.

命题 1.1. 设 $a, b, c \in \mathbb{Z}$.

(1) 如果 $c|b$, $b|a$, 那么 $c|a$.

由整除的定义, 我们不难证明下面这些基本性质.

命题 1.1. 设 $a, b, c \in \mathbb{Z}$.

(1) 如果 $c|b$, $b|a$, 那么 $c|a$.

(2) 如果 $b|a$, $c \neq 0$, 那么 $cb|ca$.

由整除的定义, 我们不难证明下面这些基本性质.

命题 1.1. 设 $a, b, c \in \mathbb{Z}$.

(1) 如果 $c|b$, $b|a$, 那么 $c|a$.

(2) 如果 $b|a$, $c \neq 0$, 那么 $cb|ca$.

(3) 如果 $c|a$, $c|b$, 那么对任意 $m, n \in \mathbb{Z}$, 有 $c|ma + nb$.

由整除的定义, 我们不难证明下面这些基本性质.

命题 1.1. 设 $a, b, c \in \mathbb{Z}$.

(1) 如果 $c|b$, $b|a$, 那么 $c|a$.

(2) 如果 $b|a$, $c \neq 0$, 那么 $cb|ca$.

(3) 如果 $c|a$, $c|b$, 那么对任意 $m, n \in \mathbb{Z}$, 有 $c|ma + nb$.

(4) 如果 $b|a$, $a|b$, 那么 $a = b$ 或 $a = -b$.

由整除的定义, 我们不难证明下面这些基本性质.

命题 1.1. 设 $a, b, c \in \mathbb{Z}$.

(1) 如果 $c|b$, $b|a$, 那么 $c|a$.

(2) 如果 $b|a$, $c \neq 0$, 那么 $cb|ca$.

(3) 如果 $c|a$, $c|b$, 那么对任意 $m, n \in \mathbb{Z}$, 有 $c|ma + nb$.

(4) 如果 $b|a$, $a|b$, 那么 $a = b$ 或 $a = -b$.

由整除的定义, 我们不难证明下面这些基本性质.

命题 1.1. 设 $a, b, c \in \mathbb{Z}$.

(1) 如果 $c|b$, $b|a$, 那么 $c|a$.

(2) 如果 $b|a$, $c \neq 0$, 那么 $cb|ca$.

(3) 如果 $c|a$, $c|b$, 那么对任意 $m, n \in \mathbb{Z}$, 有 $c|ma + nb$.

(4) 如果 $b|a$, $a|b$, 那么 $a = b$ 或 $a = -b$.

因为 $|a|$ 和 a 的所有因数都相同, 所以我们讨论因数时可以只就正整数来讨论.

下面是整除的基本定理, 也称为**带余除法**, 它是初等数论的证明中最基本, 最常用的工具.

定理 1.1. 设 $a, b \in \mathbb{Z}$, 且 $b \neq 0$, 则存在惟一的 $q, r \in \mathbb{Z}$, 使得

$$a = bq + r, \quad 0 \leq r < |b|. \tag{1}$$

例如, $a = 17, b = 5$ 时, $17 = 5 \cdot 3 + 2$, 这时 $q = 3$, $r = 2$; 而 $a = -17, b = 5$ 时, $-17 = 5 \cdot (-4) + 3$, 这时 $q = -4$, $r = 3$.

证明: (存在性) 考虑整数序列:

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

则 a 必在上述序列的某相邻两项之间, 我们不妨假定

$$q|b| \le a < (q+1)|b|.$$

于是 $0 \le a - q|b| < |b|$, 令 $r = a - q|b|$, 则有 $0 \le r < |b|$. 因此当 $b > 0$ 时, 我们有 $a = bq + r$; 当 $b < 0$ 时, 我们有 $a = b(-q) + r$. 这样, 我们就证明了 q 和 r 的存在性.

证明: (存在性) 考虑整数序列:

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

则 a 必在上述序列的某相邻两项之间, 我们不妨假定

$$q|b| \le a < (q+1)|b|.$$

于是 $0 \le a - q|b| < |b|$, 令 $r = a - q|b|$, 则有 $0 \le r < |b|$. 因此当 $b > 0$ 时, 我们有 $a = bq + r$; 当 $b < 0$ 时, 我们有 $a = b(-q) + r$. 这样, 我们就证明了 q 和 r 的存在性.

(惟一性) 假设存在另外一组 $q', r' \in \mathbb{Z}$ 使得 (1) 式成立, 即 $a = bq' + r'$, $0 \le r' < |b|$, 则有

$$-|b| < r - r' = b(q' - q) < |b|.$$

因此 $b(q' - q) = 0$, 从而 $r - r' = 0$, 即 $q' = q$, $r' = r$, 所以惟一性成立. □

定义 1.2. 我们称 (1) 式中的 q 为用 b 除 a 得出的**不完全商**, r 叫做用 b 除 a 得到的**最小非负余数**, 也简称为**余数**, 常记作 $\langle a\rangle_b$ 或 $a \bmod b$.

约定 1.1. 在不致引起混淆时, $\langle a\rangle_b$ 中的 b 常略去不写. 为方便起见, 以后除非特别说明, 我们总假定除数 b 以及因数都大于零.

作为带余除法的一个重要应用, 我们考虑整数的基 b $(b \geq 2)$ 表示. 我们知道通常所用的数都是十进制的, 计算机上用的数是 2, 8, 及 16 进制的. 下面的定理给出一个数能用不同进制表示的依据.

定理 1.2. 设 $b \geq 2$ 是给定的正整数, 那么任意正整数 n 可以惟一表示为

$$n = r_k b^k + r_{k-1} b^{k-1} + \cdots + r_1 b + r_0,$$

这里整数 $k \geq 0$, 整数 r_i $(0 \leq i \leq k)$ 满足 $0 \leq r_i < b$, $r_k \neq 0$.

定理 1.2. 设 $b \geq 2$ 是给定的正整数, 那么任意正整数 n 可以惟一表示为

$$n = r_k b^k + r_{k-1} b^{k-1} + \cdots + r_1 b + r_0,$$

这里整数 $k \geq 0$, 整数 r_i $(0 \leq i \leq k)$ 满足 $0 \leq r_i < b$, $r_k \neq 0$.

证明: 对给定的正整数 n, 必存在惟一的整数 $k \geq 0$ 使得 $b^k \leq n < b^{k+1}$. 由带余除法, 存在惟一的 $q_0, r_0 \in \mathbb{Z}$ 使得

$$n = bq_0 + r_0, \quad 0 \leq r_0 < b. \tag{2}$$

我们对 k 进行归纳证明. 当 $k = 0$ 时, 则必有 $q_0 = 0$, $1 \leq r_0 < b$, 这时结论显然成立.

假设结论对 $k = m \geq 0$ 成立. 那么当 $k = m + 1$ 时, (2) 式中的 q_0 必满足 $b^m \leq q_0 < b^{m+1}$. 由归纳假设知, q_0 可以惟一表示为

$$q_0 = s_m b^m + s_{m-1} b^{m-1} + \cdots + s_1 b + s_0,$$

其中整数 s_j $(0 \leq j \leq m)$ 满足 $0 \leq s_j < b$, $s_m \neq 0$. 因此我们有

$$n = s_m b^{m+1} + s_{m-1} b^m + \cdots + s_1 b^2 + s_0 b + r_0,$$

易见这种表示是满足定理要求的惟一表示, 否则与上面 q_0 的惟一表示性矛盾. 因此结论对 $m + 1$ 也成立. □

余数的几个基本性质

定理 1.3. 设 $a_1, a_2, b \in \mathbb{Z}$, 且 $b > 0$, 则

(1) $\langle a_1 + a_2 \rangle = \langle \langle a_1 \rangle + \langle a_2 \rangle \rangle$.

余数的几个基本性质

定理 1.3. 设 $a_1, a_2, b \in \mathbb{Z}$, 且 $b > 0$, 则

(1) $\langle a_1 + a_2 \rangle = \langle \langle a_1 \rangle + \langle a_2 \rangle \rangle$.

(2) $\langle a_1 - a_2 \rangle = \langle \langle a_1 \rangle - \langle a_2 \rangle \rangle$.

余数的几个基本性质

定理 1.3. 设 $a_1, a_2, b \in \mathbb{Z}$, 且 $b > 0$, 则

(1) $\langle a_1 + a_2 \rangle = \langle \langle a_1 \rangle + \langle a_2 \rangle \rangle$.

(2) $\langle a_1 - a_2 \rangle = \langle \langle a_1 \rangle - \langle a_2 \rangle \rangle$.

(3) $\langle a_1 a_2 \rangle = \langle \langle a_1 \rangle \langle a_2 \rangle \rangle$.

余数的几个基本性质

定理 1.3. 设 $a_1, a_2, b \in \mathbb{Z}$, 且 $b > 0$, 则

(1) $\langle a_1 + a_2 \rangle = \langle \langle a_1 \rangle + \langle a_2 \rangle \rangle$.

(2) $\langle a_1 - a_2 \rangle = \langle \langle a_1 \rangle - \langle a_2 \rangle \rangle$.

(3) $\langle a_1 a_2 \rangle = \langle \langle a_1 \rangle \langle a_2 \rangle \rangle$.

余数的几个基本性质

定理 1.3. 设 $a_1, a_2, b \in \mathbb{Z}$, 且 $b > 0$, 则

(1) $\langle a_1 + a_2 \rangle = \langle \langle a_1 \rangle + \langle a_2 \rangle \rangle$.

(2) $\langle a_1 - a_2 \rangle = \langle \langle a_1 \rangle - \langle a_2 \rangle \rangle$.

(3) $\langle a_1 a_2 \rangle = \langle \langle a_1 \rangle \langle a_2 \rangle \rangle$.

证明: (1)-(3) 证明类似, 我们仅证明 (1). 设

$a_1 = bq_1 + \langle a_1 \rangle$, $a_2 = bq_2 + \langle a_2 \rangle$,

$\langle a_1 \rangle + \langle a_2 \rangle = bq_3 + \langle \langle a_1 \rangle + \langle a_2 \rangle \rangle$. 于是

$$\begin{aligned} a_1 + a_2 &= b(q_1 + q_2) + \langle a_1 \rangle + \langle a_2 \rangle \\ &= b(q_1 + q_2 + q_3) + \langle \langle a_1 \rangle + \langle a_2 \rangle \rangle, \end{aligned}$$

因此 $\langle a_1 + a_2 \rangle = \langle \langle a_1 \rangle + \langle a_2 \rangle \rangle$, 所以断言 (1) 成立. □

定义 2.1. 设 $a_1, a_2, \ldots, a_n$ 是不全为零的整数. 如果 $d \in \mathbb{Z}$ 使得 $d|a_i$ $(1 \leq i \leq n)$, 则 d 叫做 $a_1, a_2, \ldots, a_n$ 的一个**公因数**. 公因数中最大的一个叫做**最大公因数**, 记作 $(a_1, a_2, \ldots, a_n)$. 若 $(a_1, a_2, \ldots, a_n) = 1$, 则说 $a_1, a_2, \ldots, a_n$ **互素**.

定义 2.1. 设 $a_1, a_2, \ldots, a_n$ 是不全为零的整数. 如果 $d \in \mathbb{Z}$ 使得 $d|a_i$ $(1 \leq i \leq n)$, 则 d 叫做 $a_1, a_2, \ldots, a_n$ 的一个**公因数**. 公因数中最大的一个叫做**最大公因数**, 记作 $(a_1, a_2, \ldots, a_n)$. 若 $(a_1, a_2, \ldots, a_n) = 1$, 则说 $a_1, a_2, \ldots, a_n$ **互素**.

上面的定义2.1是有意义的. 事实上, 显然 1 是 $a_1, a_2, \ldots, a_n$ 的一个公因数, 因为任意非零数的因数只有有限多个, 所以 $a_1, a_2, \ldots, a_n$ ($a_1, a_2, \ldots, a_n$ 不全为零) 的公因数也只有有限多个, 因此最大公因数 $(a_1, a_2, \ldots, a_n)$ 的确惟一存在, 并且 $(a_1, a_2, \ldots, a_n) \geq 1$.

例如, $(24, -36, 18) = 6$, $(49, 64) = 1$.

因为 $(a,1)=1$, 所以 1 与任何数均互素. 当 $a\neq 0$ 时, $(a,0)=|a|$. 更一般地, 因为 $(a_1,a_2,\ldots,a_n)=(|a_1|,|a_2|,\ldots,|a_n|)$, 又因为一组不全为零的整数的最大公因数等于它们当中全体非零整数的最大公因数, 所以不妨设 $a_i>0$ $(i=1,2,\ldots,n)$.

我们先讨论两个数的最大公因数.

定理 2.1. 设 a,b,c 是不全为零的整数, 若存在 $q\in\mathbb{Z}$ 使得 $a=bq+c$, 则 $(a,b)=(b,c)$.

因为 $(a,1)=1$, 所以 1 与任何数均互素. 当 $a\neq 0$ 时, $(a,0)=|a|$. 更一般地, 因为 $(a_1,a_2,\ldots,a_n)=(|a_1|,|a_2|,\ldots,|a_n|)$, 又因为一组不全为零的整数的最大公因数等于它们当中全体非零整数的最大公因数, 所以不妨设 $a_i>0$ $(i=1,2,\ldots,n)$.

我们先讨论两个数的最大公因数.

定理 2.1. 设 a,b,c 是不全为零的整数, 若存在 $q\in\mathbb{Z}$ 使得 $a=bq+c$, 则 $(a,b)=(b,c)$.

证明: 由 $(b,c)|b$, $(b,c)|c$ 及 $a=bq+c$ 知, $(b,c)|a$, 因此 (b,c) 是 a 和 b 的公因数. 但 (a,b) 是 a 和 b 的最大公因数, 所以 $(b,c)\leq(a,b)$. 相似地, 我们可以得到 $(a,b)\leq(b,c)$, 于是 $(a,b)=(b,c)$. □

下面的欧几里得算法, 也称作辗转相除法, 由古希腊数学家欧几里得于公元前 3 世纪提出, 它提供了一种求两个正整数的最大公因数的有效方法.

定理 2.2. 设整数 $a > 0, b > 0$. 令 $r_0 = a, r_1 = b$, 由带余除法我们不妨假设

$$\begin{aligned}
&r_0 = r_1 q_1 + r_2, \quad 0 < r_2 < r_1 \\
&r_1 = r_2 q_2 + r_3, \quad 0 < r_3 < r_2 \\
&\quad \vdots \\
&r_{n-2} = r_{n-1} q_{n-1} + r_n, \quad 0 < r_n < r_{n-1} \\
&r_{n-1} = r_n q_n,
\end{aligned} \tag{3}$$

那么 (a, b) 就是 (3) 式中最后一个非零的余数, 即 $(a, b) = r_n$.

证明： 因为 $r_1 > r_2 > r_3 > \cdots$, 所以存在 n 使得 $r_{n+1} = 0$, 从而上面的算法可以终止. 由定理2.1, 我们有

$$(a, b) = (r_0, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots$$
$$= (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

□

证明： 因为 $r_1 > r_2 > r_3 > \cdots$, 所以存在 n 使得 $r_{n+1} = 0$, 从而上面的算法可以终止. 由定理2.1, 我们有

$$(a,b) = (r_0, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots$$
$$= (r_{n-1}, r_n) = (r_n, 0) = r_n.$$ □

例 2.1. 求 $(963, 657)$.

解： 由带余除法得

$$963 = 657 \cdot 1 + 306,$$
$$657 = 306 \cdot 2 + 45,$$
$$306 = 45 \cdot 6 + 36$$
$$45 = 36 \cdot 1 + 9,$$
$$36 = 9 \cdot 4,$$

故 $(963, 657) = 9$. □

定理 2.3. 设整数 a, b 不全为零, 则存在 $s, t \in \mathbb{Z}$ 使得

$$sa + tb = (a, b). \tag{4}$$

定理 2.3. 设整数 a, b 不全为零, 则存在 $s, t \in \mathbb{Z}$ 使得

$$sa + tb = (a, b). \tag{4}$$

证明: 如果整数 a, b 有一为零, 那么结论显然成立.
下面考虑 $a > 0$, $b > 0$ 的情形. 此时, 根据带余除法, 由 (3) 式中 $r_n = r_{n-2} - r_{n-1}q_{n-1}$ 和 $r_{n-1} = r_{n-3} - r_{n-2}q_{n-2}$ 得

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

再将 $r_{n-2} = r_{n-4} - r_{n-3}q_{n-3}$ 代入上式, 如此继续下去, 最后可得 $r_n = sr_0 + tr_1$, 即 $(a, b) = sa + tb$, 其中 s, t 是两个整数.

证明 (续)

如果 $a < 0$ 或 $b < 0$, 那么对正整数 $|a|, |b|$, 由前面的证明知, 存在 $s', t' \in \mathbb{Z}$ 使得 $s'|a| + t'|b| = (a, b)$, 所以存在 $s, t \in \mathbb{Z}$ 使得 $sa + tb = (a, b)$. 因此定理成立. □

注意, 满足 (4) 式的 s, t 可能不惟一. 一个简单的例子是

$$(4, 2) = 1 \cdot 4 + (-1) \cdot 2 = 2 \cdot 4 + (-3) \cdot 2.$$

例 2.2. 求一组整数 s, t 使得

$$963s + 657t = (963, 657).$$

例 2.2. 求一组整数 s, t 使得

$$963s + 657t = (963, 657).$$

解: 由例2.1的求解得

$$\begin{aligned}(963, 657) = 9 &= 45 - 36 \cdot 1 \\ &= 45 - (306 - 45 \cdot 6) \cdot 1 = 45 \cdot 7 - 306 \cdot 1 \\ &= (657 - 306 \cdot 2) \cdot 7 - 306 = 306(-15) + 657 \cdot 7 \\ &= (963 - 657 \cdot 1) \cdot (-15) + 657 \cdot 7 \\ &= (-15) \cdot 963 + 22 \cdot 657,\end{aligned}$$

因此取 $s = -15$, $t = 22$ 可满足

$963s + 657t = (963, 657).$ □

特别地, 当 a, b 互素时, 由定理2.3我们有下面的结论.

推论 2.1. 设整数 a, b 不全为零, 则 $(a, b) = 1$ 当且仅当存在 $s, t \in \mathbb{Z}$ 使得 $sa + tb = 1$.

特别地, 当 a, b 互素时, 由定理2.3我们有下面的结论.

推论 2.1. 设整数 a, b 不全为零, 则 $(a, b) = 1$ 当且仅当存在 $s, t \in \mathbb{Z}$ 使得 $sa + tb = 1$.

作为定理2.3的推论, 我们易见 a, b 的任意公因数一定是它们最大公因数的因数.

推论 2.2. 如果 $d|a$, 且 $d|b$, 那么 $d|(a, b)$.

特别地, 当 a, b 互素时, 由定理2.3我们有下面的结论.

推论 2.1. 设整数 a, b 不全为零, 则 $(a, b) = 1$ 当且仅当存在 $s, t \in \mathbb{Z}$ 使得 $sa + tb = 1$.

作为定理2.3的推论, 我们易见 a, b 的任意公因数一定是它们最大公因数的因数.

推论 2.2. 如果 $d|a$, 且 $d|b$, 那么 $d|(a, b)$.

命题 2.1. 设 $a, b, c \in \mathbb{Z}$, 则 $(ac, bc) = (a, b)|c|$.

证明: 因为用 $|c|$ 乘 (3) 式中各式, (3) 式中 r_i $(0 \leq i \leq n)$ 就变成了 $r_i|c|$, 所以由定理2.2知 $(ac, bc) = (a, b)|c|$. □

例如, $(48, 36) = (4, 3) \cdot 12 = 12$.

由命题2.1, 我们有如下推论.

推论 2.3. 设 d 是一正整数, 那么 $d = (a, b)$ 的充要条件是 $(a/d, b/d) = 1$.

由命题2.1, 我们有如下推论.

推论 2.3. 设 d 是一正整数, 那么 $d=(a,b)$ 的充要条件是 $(a/d,b/d)=1$.

证明: 由命题2.1知

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

因此, 如果 $d=(a,b)$, 那么 $(a/d,b/d)=1$; 反过来, 如果 $(a/d,b/d)=1$, 那么 $d=(a,b)$. □

利用上面推论的充分性, 可以判断一个数 d 是否是 a,b 的最大公因数.

下面的命题给出另外一种判断方法.

命题 2.2. 设 d 是一正整数, a, b 是不全为零的整数, 则 $d = (a, b)$ 的充要条件是

(1) $d|a$, 且 $d|b$;

下面的命题给出另外一种判断方法.

命题 2.2. 设 d 是一正整数, a, b 是不全为零的整数, 则 $d = (a, b)$ 的充要条件是

(1) $d|a$, 且 $d|b$;

(2) 如果 $c \in \mathbb{Z}$ 满足 $c|a$ 和 $c|b$, 那么 $c|d$.

下面的命题给出另外一种判断方法.

命题 2.2. 设 d 是一正整数, a, b 是不全为零的整数, 则 $d = (a, b)$ 的充要条件是

(1) $d|a$, 且 $d|b$;

(2) 如果 $c \in \mathbb{Z}$ 满足 $c|a$ 和 $c|b$, 那么 $c|d$.

下面的命题给出另外一种判断方法.

命题 2.2. 设 d 是一正整数, a, b 是不全为零的整数, 则 $d = (a, b)$ 的充要条件是

(1) $d|a$, 且 $d|b$;

(2) 如果 $c \in \mathbb{Z}$ 满足 $c|a$ 和 $c|b$, 那么 $c|d$.

证明: 由推论2.2, 必要性显然成立. 下面考虑充分性. 由条件 (1) 知, d 是 a, b 的公因数, 因此 $d \leq (a, b)$. 另一方面, 由条件 (2) 我们得到 $(a, b)|d$, 所以 $(a, b) \leq d$, 于是 $d = (a, b)$, 从而充分性成立. □

命题 2.3. 如果 $(a, b) = 1$, 那么 $(a, bc) = (a, c)$.

命题 2.3. 如果 $(a,b)=1$, 那么 $(a,bc)=(a,c)$.

证明: 因为 $(a,bc)|ac$, $(a,bc)|bc$, 所以 $(a,bc)|(ac,bc)$. 而由命题2.1知 $(ac,bc)=(a,b)|c|=|c|$, 因此 $(a,bc)|c$. 又因为 $(a,bc)|a$, 所以 $(a,bc)|(a,c)$. 反过来, 显然有 $(a,c)|a$, $(a,c)|bc$, 因此 $(a,c)|(a,bc)$, 于是 $(a,bc)=(a,c)$. □

例如, $(20,973\cdot 15)=(20,15)=5$.

由命题2.3我们很容易得出下面几个常用的结果.

推论 2.4.

(1) 如果 $(a,b)=1$, $a|bc$, 那么 $a|c$.

推论 2.4.

(1) 如果 $(a,b)=1$, $a|bc$, 那么 $a|c$.

(2) 如果 $(a,b)=1$, $a|c$, $b|c$, 那么 $ab|c$.

推论 2.4.

(1) 如果 $(a,b)=1$, $a|bc$, 那么 $a|c$.

(2) 如果 $(a,b)=1$, $a|c$, $b|c$, 那么 $ab|c$.

(3) 如果 $(a,b)=1$, $(a,c)=1$, 那么 $(a,bc)=1$.

推论 2.4.

(1) 如果 $(a,b)=1$, $a|bc$, 那么 $a|c$.

(2) 如果 $(a,b)=1$, $a|c$, $b|c$, 那么 $ab|c$.

(3) 如果 $(a,b)=1$, $(a,c)=1$, 那么 $(a,bc)=1$.

推论 2.4.

(1) 如果 $(a,b)=1$, $a|bc$, 那么 $a|c$.

(2) 如果 $(a,b)=1$, $a|c$, $b|c$, 那么 $ab|c$.

(3) 如果 $(a,b)=1$, $(a,c)=1$, 那么 $(a,bc)=1$.

证明: (1) 由条件及命题2.3我们有 $(a,c)=(a,bc)=a$, 因此 $a|c$.

推论 2.4.

(1) 如果 $(a,b)=1$, $a|bc$, 那么 $a|c$.

(2) 如果 $(a,b)=1$, $a|c$, $b|c$, 那么 $ab|c$.

(3) 如果 $(a,b)=1$, $(a,c)=1$, 那么 $(a,bc)=1$.

证明: (1) 由条件及命题2.3我们有 $(a,c)=(a,bc)=a$, 因此 $a|c$.

(2) 因为 $b|c$, 所以存在 $d\in\mathbb{Z}$ 使得 $c=bd$. 由 $a|c$ 知 $a|bd$, 进而由 (1) 得 $a|d$, 于是 $ab|bd$, 即 $ab|c$.

推论 2.4.

(1) 如果 $(a,b)=1$, $a|bc$, 那么 $a|c$.

(2) 如果 $(a,b)=1$, $a|c$, $b|c$, 那么 $ab|c$.

(3) 如果 $(a,b)=1$, $(a,c)=1$, 那么 $(a,bc)=1$.

证明: (1) 由条件及命题2.3我们有 $(a,c)=(a,bc)=a$, 因此 $a|c$.

(2) 因为 $b|c$, 所以存在 $d\in\mathbb{Z}$ 使得 $c=bd$. 由 $a|c$ 知 $a|bd$, 进而由 (1) 得 $a|d$, 于是 $ab|bd$, 即 $ab|c$.

(3) 由命题2.3, 我们有 $(a,bc)=(a,c)=1$. □

下面的定理提供了求 n $(n \geq 3)$ 个数的最大公因数的方法.

定理 2.4. 设 $a_1, a_2, \ldots, a_n$ 是 n 个不全为零的整数, 则

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2), a_3, \ldots, a_n). \tag{5}$$

下面的定理提供了求 n $(n \geq 3)$ 个数的最大公因数的方法.

定理 2.4. 设 $a_1, a_2, \ldots, a_n$ 是 n 个不全为零的整数, 则

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2), a_3, \ldots, a_n). \tag{5}$$

证明: 由推论2.2知, $a_1, a_2, \ldots, a_n$ 的任意公因数一定是 $(a_1, a_2), a_3, \ldots, a_n$ 的公因数; 反过来, $(a_1, a_2), a_3, \ldots, a_n$ 的任意公因数一定是 $a_1, a_2, \ldots, a_n$ 的公因数. 由此可见, $a_1, a_2, \ldots, a_n$ 和 $(a_1, a_2), a_3, \ldots, a_n$ 必有相同的最大公因数, 即 $(a_1, a_2, \ldots, a_n) = ((a_1, a_2), a_3, \ldots, a_n)$. □

下面的定理提供了求 n $(n \geq 3)$ 个数的最大公因数的方法.

定理 2.4. 设 $a_1, a_2, \ldots, a_n$ 是 n 个不全为零的整数, 则

$$(a_1, a_2, \ldots, a_n) = ((a_1, a_2), a_3, \ldots, a_n). \tag{5}$$

证明: 由推论2.2知, $a_1, a_2, \ldots, a_n$ 的任意公因数一定是 $(a_1, a_2), a_3, \ldots, a_n$ 的公因数; 反过来, $(a_1, a_2), a_3, \ldots, a_n$ 的任意公因数一定是 $a_1, a_2, \ldots, a_n$ 的公因数. 由此可见, $a_1, a_2, \ldots, a_n$ 和 $(a_1, a_2), a_3, \ldots, a_n$ 必有相同的最大公因数, 即 $(a_1, a_2, \ldots, a_n) = ((a_1, a_2), a_3, \ldots, a_n)$. □

作为定理2.3的推广, 我们有下面的结果.

定理 2.5. 设整数 $a_1, a_2, \ldots, a_n$ 不全为零, 则存在 $s_1, s_2, \ldots, s_n \in \mathbb{Z}$ 使得

$$s_1 a_1 + s_2 a_2 + \cdots + s_n a_n = (a_1, a_2, \ldots, a_n).$$

定义 3.1. 设 $a_1, a_2, \ldots, a_n$ 是全不为零的整数, 若 $a_i | m$ $(1 \leq i \leq n)$, 则称 m 为这 n 个数的一个**公倍数**. $a_1, a_2, \ldots, a_n$ 的所有公倍数中最小的正公倍数称为这 n 个数的**最小公倍数**, 记作 $[a_1, a_2, \ldots, a_n]$.

定义 3.1. 设 $a_1, a_2, \ldots, a_n$ 是全不为零的整数, 若 $a_i | m$ $(1 \leq i \leq n)$, 则称 m 为这 n 个数的一个**公倍数**. $a_1, a_2, \ldots, a_n$ 的所有公倍数中最小的正公倍数称为这 n 个数的**最小公倍数**, 记作 $[a_1, a_2, \ldots, a_n]$.

因为 $|a_1 a_2 \cdots a_n|$ 就是 $a_1, a_2, \ldots, a_n$ 的一个正公倍数, 所以最小公倍数存在. 另外, 由于任何正整数都不是 0 的倍数, 因此讨论最小公倍数时总假定这些整数均不为零. 又因为 $[a_1, a_2, \ldots, a_n] = [|a_1|, |a_2|, \ldots, |a_n|]$, 所以我们可以只对正整数讨论它们的最小公倍数.

定理 3.1. 整数 a, b 的公倍数是它们的最小公倍数的倍数.

定理 3.1. 整数 a, b 的公倍数是它们的最小公倍数的倍数.

证明: 设 k 是 a, b 的一个公倍数, 并假设用 $m = [a, b]$ 除 k 得

$$k = mq + r, \quad 0 \leq r < m.$$

因为 $a|k$, $a|m$, 所以 $a|r$. 同理, 我们有 $b|r$, 所以 r 是 a, b 的一个倍数. 因为 $0 \leq r < m$, 且 m 是 a, b 的最小公倍数, 所以 $r = 0$, 即 $k = mq$. 因此定理成立. □

由定理3.1, 显然有 $\{a, b\text{的公倍数}\} = \{k[a, b] | k \in \mathbb{Z}\}$.

命题 3.1. 设 m 是一正整数, a, b 是全不为零的整数, 则 $m = [a, b]$ 的充要条件是

(1) $a|m$, 且 $b|m$;

命题 3.1. 设 m 是一正整数, a, b 是全不为零的整数, 则 $m = [a, b]$ 的充要条件是

(1) $a|m$, 且 $b|m$;

(2) 如果 $n \in \mathbb{Z}$ 满足 $a|n$ 和 $b|n$, 那么 $m|n$.

命题 3.1. 设 m 是一正整数, a, b 是全不为零的整数, 则 $m = [a, b]$ 的充要条件是

(1) $a|m$, 且 $b|m$;

(2) 如果 $n \in \mathbb{Z}$ 满足 $a|n$ 和 $b|n$, 那么 $m|n$.

命题 3.1. 设 m 是一正整数, a, b 是全不为零的整数, 则 $m = [a, b]$ 的充要条件是

(1) $a|m$, 且 $b|m$;

(2) 如果 $n \in \mathbb{Z}$ 满足 $a|n$ 和 $b|n$, 那么 $m|n$.

证明: 由定理3.1, 必要性显然成立. 下面考虑充分性. 由条件 (1) 知, m 是 a, b 的公倍数, 因此 $[a, b] \leq m$. 另一方面, 由条件 (2) 我们得到 $m|[a, b]$, 所以 $m \leq [a, b]$, 于是 $m = [a, b]$, 从而充分性成立. □

定理 3.2. 如果整数 a, b 均不为零, 那么

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

定理 3.2. 如果整数 a, b 均不为零, 那么

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

证明: 为了简单起见, 假设 $[a, b] = m$, $(a, b) = d$. 因为 $a|m$, 所以 $ab|mb$; 同理, 因为 $b|m$, 所以 $ab|ma$. 因此 $ab|(ma, mb)$, 所以 $ab|m(a, b)$, 即 $ab|md$.
另一方面, 我们有 $a|\frac{ab}{d}$, $b|\frac{ab}{d}$, 即 $\frac{ab}{d}$ 是 a, b 的一个公倍数. 由定理3.1, 我们有 $m|\frac{ab}{d}$, 因此 $md|ab$, 从而 $md = ab$ 或 $md = -ab$, 即 $md = |ab|$, 所以定理成立. □

定理3.2表明求最小公倍数可以转化为求最大公因数. 例如,

$$[48, -32] = \frac{48 \cdot 32}{(48, -32)} = \frac{48 \cdot 32}{16(3, -2)} = 96.$$

定理 3.3. 设 $a_1, a_2, \ldots, a_n$ 是 n 个全不为零的整数, 则

$$[a_1, a_2, \ldots, a_n] = [[a_1, a_2], a_3, \ldots, a_n].$$

定理 3.3. 设 $a_1, a_2, \ldots, a_n$ 是 n 个全不为零的整数, 则

$$[a_1, a_2, \ldots, a_n] = [[a_1, a_2], a_3, \ldots, a_n].$$

证明: 由定理3.1知, $a_1, a_2, \ldots, a_n$ 的任意公倍数一定是 $[a_1, a_2], a_3, \ldots, a_n$ 的公倍数; 反过来, $[a_1, a_2], a_3, \ldots, a_n$ 的任意公倍数一定是 $a_1, a_2, \ldots, a_n$ 的公倍数. 因此, $a_1, a_2, \ldots, a_n$ 和 $[a_1, a_2], a_3, \ldots, a_n$ 必有相同的最小公倍数, 即 $[a_1, a_2, \ldots, a_n] = [[a_1, a_2], a_3, \ldots, a_n]$. □

借助定理3.3, 定理3.2中的公式可以推广到任意多个数的情形.

命题 3.2. 设整数 a, b, c 均不为零, 则

$$[a, b, c] = \frac{|abc|}{(ab, ac, bc)}.$$

借助定理3.3, 定理3.2中的公式可以推广到任意多个数的情形.

命题 3.2. 设整数 a, b, c 均不为零, 则

$$[a, b, c] = \frac{|abc|}{(ab, ac, bc)}.$$

证明: 反复使用定理3.2, 我们有

$$\begin{aligned}
[a, b, c] &= [[a, b], c] = \frac{[a, b]|c|}{([a, b], c)} \\
&= \frac{|abc|}{(a, b)([a, b], c)} = \frac{|abc|}{(ab, (a, b)c)} \\
&= \frac{|abc|}{(ab, ac, bc)}.
\end{aligned}$$

故得证. □

不定方程是一类特殊的方程, 其特点是方程的个数少于未知数的个数, 且它的解受到某种限制 (如整数或正整数等). 三世纪初, 古希腊数学家丢番图 (Diophantus of Alexandria) 曾大力研究过这类方程, 因此不定方程也叫做**丢番图方程**.

设整数 $k \geq 2$, $a_1, a_2, \ldots, a_k, c \in \mathbb{Z}$, 且 $a_1, a_2, \ldots, a_k$ 均不为零, 未知数 $x_1, x_2, \ldots, x_k$ 取值为整数的方程

$a_1x_1 + a_2x_2 + \cdots + a_kx_k = c$ 称为 k 元**一次不定方程**,

$a_1, a_2, \ldots, a_k$ 称为它的系数.

定理 4.1. 设 $a, b, c \in \mathbb{Z}$, a, b 均不为零, $d = (a, b)$.

(1) 二元一次不定方程

$$ax + by = c \tag{6}$$

有整数解当且仅当 $d|c$.

定理 4.1. 设 $a, b, c \in \mathbb{Z}$, a, b 均不为零, $d = (a, b)$.

(1) 二元一次不定方程

$$ax + by = c \tag{6}$$

有整数解当且仅当 $d|c$.

(2) 当方程 (6) 有解时, 它的解与不定方程

$$\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d} \tag{7}$$

的解相同.

定理 4.1. 设 $a, b, c \in \mathbb{Z}$, a, b 均不为零, $d = (a, b)$.

(1) 二元一次不定方程

$$ax + by = c \tag{6}$$

有整数解当且仅当 $d|c$.

(2) 当方程 (6) 有解时, 它的解与不定方程

$$\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d} \tag{7}$$

的解相同.

(3) 如果 $x = x_0$, $y = y_0$ 是 (6) 的一组特解, 那么它的全部解可表为

$$x = x_0 + \frac{b}{d}t, \quad y = y_0 - \frac{a}{d}t,$$

其中 t 为任意整数.

(1) $ax + by = c$ 有整数解当且仅当 $d|c$

(1) 如果 (6) 有整数解, 那么显然有 $(a, b)|c$, 即 $d|c$. 反过来, 假设 $(a, b)|c$, 则存在 $k \in \mathbb{Z}$ 使得 $c = k(a, b)$. 由定理2.3知, 存在 $s, t \in \mathbb{Z}$ 使得 $sa + tb = (a, b)$, 因此有 $ksa + ktb = k(a, b) = c$, 这表明 (6) 有整数解 $x = ks$, $y = kt$.

(1) $ax + by = c$ 有整数解当且仅当 $d|c$

(1) 如果 (6) 有整数解, 那么显然有 $(a, b)|c$, 即 $d|c$. 反过来, 假设 $(a, b)|c$, 则存在 $k \in \mathbb{Z}$ 使得 $c = k(a, b)$. 由定理2.3知, 存在 $s, t \in \mathbb{Z}$ 使得 $sa + tb = (a, b)$, 因此有 $ksa + ktb = k(a, b) = c$, 这表明 (6) 有整数解 $x = ks$, $y = kt$.

(2) 直接验证：(6) 有解时, 它的解与不定方程 $\frac{a}{d}x + \frac{b}{d}y = \frac{c}{d}$ 的解相同.

(3) 如果 $x = x_0, y = y_0$ 是 (6) 的一组特解, 那么它的全部解可表为 $x = x_0 + \frac{b}{d}t,\ y = y_0 - \frac{a}{d}t$

(3) 如果 $x = x_0, y = y_0$ 是 (6) 的一组特解, 则有 $ax_0 + by_0 = c$, 于是对任意整数 t, 将 $x = x_0 + \frac{b}{d}t, y = y_0 - \frac{a}{d}t$ 代入 (6) 知, 它们的确是 (6) 的解. 设 x, y 是 (6) 的任一组解, 则有 $ax + by = c$, 与 $ax_0 + by_0 = c$ 相减得 $a(x - x_0) = b(y_0 - y)$, 从而 $\frac{a}{d}(x - x_0) = \frac{b}{d}(y_0 - y)$.
因为 $(\frac{a}{d}, \frac{b}{d}) = 1$, 所以 $\frac{a}{d} | y_0 - y$, 故存在 $t \in \mathbb{Z}$ 使得 $y_0 - y = \frac{a}{d}t$, 即 $y = y_0 - \frac{a}{d}t$, 从而有 $x = x_0 + \frac{b}{d}t$. 因此 (6) 的全部解都可表为 $x = x_0 + \frac{b}{d}t, y = y_0 - \frac{a}{d}t$ 的形式, 所以定理成立. □

特别地, 如果 $(a,b)=1$, 那么 (6) 的任一解都可表为 $x=x_0+bt, y=y_0-at$ 的形式, 这里 $t\in\mathbb{Z}$, x_0,y_0 是 (6) 的一组特解.

特别地, 如果 $(a,b)=1$, 那么 (6) 的任一解都可表为 $x=x_0+bt, y=y_0-at$ 的形式, 这里 $t\in\mathbb{Z}$, x_0,y_0 是 (6) 的一组特解.

例 4.1. 求二元一次不定方程

$$963x+657y=18 \tag{8}$$

的整数解.

特别地, 如果 $(a,b)=1$, 那么 (6) 的任一解都可表为 $x=x_0+bt, y=y_0-at$ 的形式, 这里 $t\in\mathbb{Z}$, x_0,y_0 是 (6) 的一组特解.

例 4.1. 求二元一次不定方程

$$963x+657y=18 \tag{8}$$

的整数解.

解: 由例2.1, 我们有 $(963,657)=9$. 因为 $9|18$, 所以由定理4.1知, (8) 必有整数解.

在例2.2中, 我们已经发现

$963\cdot(-15)+657\cdot 22=(963,657)=9$, 因此 $x_0=-30$, $y_0=44$ 是 (8) 的一组特解. 进而由定理4.1知, (8) 的所有整数解为 $x=-30+73t,\quad y=44-107t$, 其中 $t\in\mathbb{Z}$. □

欧拉曾经研究过下面的问题.

例 4.2. 一个农场主计划用 1770 克朗购买牛和马, 牛每头 21 克朗, 马每头 31 克朗, 问他可以买多少牛和马?

欧拉曾经研究过下面的问题.

例 4.2. 一个农场主计划用 1770 克朗购买牛和马, 牛每头 21 克朗, 马每头 31 克朗, 问他可以买多少牛和马?

解: 设可以买 x 头牛, y 头马, 则原问题等价于求二元一次不定方程

$$21x + 31y = 1770 \tag{9}$$

的正整数解. 因为 $(21, 31) = 1$, 所以由欧几里得算法得 $3 \cdot 21 + (-2) \cdot 31 = 1$, 故 $x_0 = 3 \cdot 1770 = 5310$, $y_0 = (-2) \cdot 1770 = -3540$ 是 (9) 的一组特解, 从而 (9) 的一般解为 $x = 5310 + 31t$, $y = -3540 - 21t$, 其中 $t \in \mathbb{Z}$. 因此, (9) 的正整数解要求

$$\begin{cases} 5310 + 31t > 0 \\ -3540 - 21t > 0. \end{cases}$$

解之得 $t = -169, -170,$ 或 $-171,$ 从而得到 (9) 的三组正整数解

$$\begin{cases} x = 71 \\ y = 9, \end{cases} \quad \begin{cases} x = 40 \\ y = 30, \end{cases} \quad \begin{cases} x = 9 \\ y = 51, \end{cases}$$

即该农场主可以买 71 头牛, 9 头马, 或者买 40 头牛, 30 头马, 或者买 9 头牛, 51 头马. □

当二元一次不定方程的系数不太大时, 有时我们可以用观察法求其特解. 此外, 我们还可以用下面逐渐减小系数的方法.

例 4.3. 求二元一次不定方程

$$7x + 19y = 213 \tag{10}$$

的整数解.

当二元一次不定方程的系数不太大时, 有时我们可以用观察法求其特解. 此外, 我们还可以用下面逐渐减小系数的方法.

例 4.3. 求二元一次不定方程

$$7x + 19y = 213 \tag{10}$$

的整数解.

解: 因为 $(7, 19)|213$, 所以 (10) 有整数解. 用最小的系数 7 除方程 (10) 两边得 $x = \frac{213-19y}{7} = 30 - 2y + \frac{3-5y}{7}$. 令 $\frac{3-5y}{7} = z$. 因为 x, y 均为整数, 所以 z 也是整数, 即有二元一次不定方程 $5y + 7z = 3$. 又用 5 除上式两边得 $y = \frac{3-7z}{5} = -z + \frac{3-2z}{5}$. 令 $\frac{3-2z}{5} = s$ 得 $2z + 5s = 3$. 显然 $z = -1$, $s = 1$ 是它的一组特解, 所以 $x = 25$, $y = 2$ 是 (10) 的一组特解, 于是 (10) 的一般解为

$x = 25 + 19t$, $y = 2 - 7t$, 其中 $t \in \mathbb{Z}$. □

对于三元或多元一次不定方程, 我们有下面的定理.

定理 4.2. k 元一次不定方程

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = c \tag{11}$$

有整数解的充要条件是 $d|c$, 这里 $d = (a_1, a_2, \ldots, a_k)$.

对于三元或多元一次不定方程, 我们有下面的定理.

定理 4.2. k 元一次不定方程

$$a_1x_1 + a_2x_2 + \cdots + a_kx_k = c \tag{11}$$

有整数解的充要条件是 $d|c$, 这里 $d = (a_1, a_2, \ldots, a_k)$.

证明: 必要性是显然的, 下面只证明充分性. 由定理2.5知, 存在 $s_1, s_2, \ldots, s_k \in \mathbb{Z}$ 使得

$$s_1a_1 + s_2a_2 + \cdots + s_ka_k = d.$$

设 $c = de$, 则易见 $x_1 = s_1e$, $x_2 = s_2e$, $\ldots$, $x_k = s_ke$ 是方程 (11) 的一组整数解, 所以定理成立. □

因为方程 (11) 的一般解比较复杂, 所以我们在此不作讨论.

在实际求解多元不定方程时, 我们可以采用与二元不定方程类似的方法.

例 4.4. 求不定方程 $50x + 45y + 36z = 10$ 的整数解.

在实际求解多元不定方程时, 我们可以采用与二元不定方程类似的方法.

例 4.4. 求不定方程 $50x + 45y + 36z = 10$ 的整数解.

解: 我们可以将它分成下面两个二元一次不定方程来求解: $50x + 45y = 5t$, $5t + 36z = 10$. 因为 $50 \cdot t + 45 \cdot (-t) = 5t$, $5 \cdot (-70) + 36 \cdot 10 = 10$, 所以上面两个方程的解分别为

$$\begin{cases} x = t + 9k \\ y = -t - 10k, \end{cases} \qquad \begin{cases} t = -70 + 36l \\ z = 10 - 5l, \end{cases}$$

这里 $k, l \in \mathbb{Z}$. 消去 t 就得到所求解

$$\begin{cases} x = -70 + 9k + 36l \\ y = 70 - 10k - 36l \\ z = 10 - 5l, \end{cases}$$

其中 $k, l \in \mathbb{Z}$.

我们也可以同例4.3一样用逐渐减小系数的方法求解.

因为 36 是所给方程系数中最小的, 我们可以把所给方程写成

$$36(x+y+z)+14x+9y=10,$$

令 $x+y+z=k$, 得 $14x+9y+36k=10$,

从而有 $9(x+y+4k)+5x=10$.

令 $x+y+4k=5l$, 得 $5x+45l=10$, 即 $x+9l=2$. 于是得所求解

$$\begin{cases} x=2-9l \\ y=-2-4k+14l \\ z=5k-5l, \end{cases}$$

其中 $k,l\in\mathbb{Z}$. 不难验证, 前后两组解是一致的. □

定义 5.1. 设 $p \in \mathbb{Z}$, $p > 1$. 如果 p 的正因数只有 1 和 p, 则 p 叫做一个**素数**; 否则, p 叫做一个**合数**.

定义 5.1. 设 $p \in \mathbb{Z}$, $p > 1$. 如果 p 的正因数只有 1 和 p, 则 p 叫做一个**素数**; 否则, p 叫做一个**合数**.

命题 5.1. 每个大于 1 的正整数都有一个素因数.

定义 5.1. 设 $p \in \mathbb{Z}$, $p > 1$. 如果 p 的正因数只有 1 和 p, 则 p 叫做一个**素数**; 否则, p 叫做一个**合数**.

命题 5.1. 每个大于 1 的正整数都有一个素因数.

证明: (反证法) 假设 a (> 1) 是最小的没有素因数的正整数. 那么 a 不可能是素数, 因此可设 $a = bc$, 其中 $1 < b < a$, $1 < c < a$. 因为 $b < a$, 所以由假设 b 有素因数, 记作 p. 由 $p|b$ 及 $b|a$ 知, 我们有 $p|a$, 这与假设矛盾. 因此结论成立. □

命题 5.2. 对任意素数 p 和整数 a, 有 $p|a$ 或 $(p,a)=1$.

命题 5.2. 对任意素数 p 和整数 a, 有 $p|a$ 或 $(p,a)=1$.

证明: 因为 $(p,a)|p$, 所以由素数定义知 $(p,a)=1$ 或 $(p,a)=p$, 而后者等价于 $p|a$, 因此命题成立. □

命题 5.2. 对任意素数 p 和整数 a, 有 $p|a$ 或 $(p,a)=1$.

证明: 因为 $(p,a)|p$, 所以由素数定义知 $(p,a)=1$ 或 $(p,a)=p$, 而后者等价于 $p|a$, 因此命题成立. □

命题 5.3. 设 p 是素数, 如果 $p|ab$, 则 $p|a$ 或 $p|b$.

命题 5.2. 对任意素数 p 和整数 a, 有 $p|a$ 或 $(p,a)=1$.

证明: 因为 $(p,a)|p$, 所以由素数定义知 $(p,a)=1$ 或 $(p,a)=p$, 而后者等价于 $p|a$, 因此命题成立. □

命题 5.3. 设 p 是素数, 如果 $p|ab$, 则 $p|a$ 或 $p|b$.

证明: 如果 $p|a$, 那么结论成立. 否则, 由命题5.2知 $(p,a)=1$. 于是由推论2.4有 $p|b$, 所以命题成立. □

定理 5.1 (算术基本定理). 设整数 $a > 1$, 则 a 能被惟一分解为

$$a = p_1 p_2 \cdots p_n,$$

其中 p_i $(1 \leq i \leq n)$ 是满足 $p_1 \leq p_2 \leq \cdots \leq p_n$ 的素数.

定理 5.1 (算术基本定理). 设整数 $a > 1$, 则 a 能被惟一分解为

$$a = p_1 p_2 \cdots p_n,$$

其中 p_i $(1 \le i \le n)$ 是满足 $p_1 \le p_2 \le \cdots \le p_n$ 的素数.

证明: 我们先证明分解的存在性. 如果 a 是素数, 取 $p_1 = a$ 即可. 如果 a 是合数, 那么由命题5.1, a 的大于 1 的最小因数, 记作 p_1, 必是素数. 设 $a = p_1 q_2$, 如果 q_2 是素数, 取 $p_2 = q_2$; 否则, 我们可取 p_2 为 q_2 的大于 1 的最小因数, 且设 $q_2 = p_2 q_3$. 同理, 可根据 q_3 取 p_3, 依次下去取 $p_4, \ldots, p_i, \ldots$, 因为 $a > q_2 > q_3 > \cdots$, 所以该过程必终止. 假设在第 n 步终止, 则由 p_i 的取法有 $a = p_1 p_2 \cdots p_n$, 且易见 $p_1 \le p_2 \le \cdots \le p_n$.

下面证明分解的惟一性: 假设存在大于 1 的整数 a 有两个不同的分解, 不妨假设 a 是有两个不同的分解的数中最小的. 设

$$a = p_1 p_2 \cdots p_n = q_1 q_2 \cdots q_m,$$

其中 p_i $(1 \le i \le n)$ 是满足 $p_1 \le p_2 \le \cdots \le p_n$ 的素数, q_i $(1 \le i \le m)$ 是满足 $q_1 \le q_2 \le \cdots \le q_m$ 的素数, 则有 $p_1 \ne q_1$, 否则 a 不是最小的有两个不同分解的正整数. 因为 $p_1 | q_1 q_2 \cdots q_m$, 所以由命题5.3存在 q_i $(i > 1)$ 使得 $p_1 | q_i$. 因为 q_i 是素数, 所以 $p_1 = q_i$. 由 $q_i \ge q_1$, 我们有 $p_1 \ge q_1$. 同理, 我们可以得到 $q_1 \ge p_1$, 因此 $p_1 = q_1$, 矛盾! 故满足要求的分解是惟一的. □

如果把算术基本定理中 $a = p_1 p_2 \cdots p_n$ 里相同的素数集中, 我们就得到

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \tag{12}$$

这里 α_i $(1 \leq i \leq k)$, $p_1 < p_2 < \cdots < p_k$. 式 (12) 叫做 a 的**标准分解式**.

例如, 72 的标准分解式是 $2^3 \cdot 3^2$, 100 的标准分解式是 $2^2 \cdot 5^2$.

如果把算术基本定理中 $a = p_1 p_2 \cdots p_n$ 里相同的素数集中, 我们就得到

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, \tag{12}$$

这里 α_i $(1 \le i \le k)$, $p_1 < p_2 < \cdots < p_k$. 式 (12) 叫做 a 的**标准分解式**.

例如, 72 的标准分解式是 $2^3 \cdot 3^2$, 100 的标准分解式是 $2^2 \cdot 5^2$.

如果一个正整数 $d|a$, 那么由式 (12) 和命题5.3知, d 可以表示为

$$d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}, \quad 0 \le \beta_i \le \alpha_i \ (1 \le i \le k). \tag{13}$$

反过来, 如果一个正整数 d 可表为 (13) 的形式, 则必有 $d|a$.

例 5.1. 证明: 如果 $a^2|b^2$, 那么 $a|b$.

例 5.1. 证明: 如果 $a^2|b^2$, 那么 $a|b$.

证明: 不妨假设 a, b 均是正整数, 且 $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, 其中 $\alpha_i \geq 0, \beta_i \geq 0$ $(1 \leq i \leq k)$. 因为 $a^2|b^2$, 所以存在 $q \in \mathbb{Z}$ 使得 $b^2 = a^2 q$, 即

$$p_1^{2\beta_1} p_2^{2\beta_2} \cdots p_k^{2\beta_k} = p_1^{2\alpha_1} p_2^{2\alpha_2} \cdots p_k^{2\alpha_k} q.$$

由此可见, $2\alpha_i \leq 2\beta_i$ $(1 \leq i \leq k)$, 即 $\alpha_i \leq \beta_i$ $(1 \leq i \leq k)$, 因此有 $a|b$. □

标准分解式也可用于刻画最大公因数和最小公倍数.

命题 5.4. 设 $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, 其中 $\alpha_i \geq 0, \beta_i \geq 0$ $(1 \leq i \leq k)$, 则

$$(a,b) = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}, \quad s_i = \min(\alpha_i, \beta_i) \ (1 \leq i \leq k);$$
$$[a,b] = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}, \quad t_i = \max(\alpha_i, \beta_i) \ (1 \leq i \leq k).$$

证明: 直接由定义即得. □

标准分解式也可用于刻画最大公因数和最小公倍数.

命题 5.4. 设 $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$, 其中 $\alpha_i \geq 0, \beta_i \geq 0$ $(1 \leq i \leq k)$, 则

$$(a,b) = p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k}, \quad s_i = \min(\alpha_i, \beta_i) \ (1 \leq i \leq k);$$
$$[a,b] = p_1^{t_1} p_2^{t_2} \cdots p_k^{t_k}, \quad t_i = \max(\alpha_i, \beta_i) \ (1 \leq i \leq k).$$

证明: 直接由定义即得. □

例如, 当 $a = 72 = 2^3 \cdot 3^2$, $b = 100 = 2^2 \cdot 5^2$ 时, 有 $(a,b) = 2^2$, $[a,b] = 2^3 \cdot 3^2 \cdot 5^2$.

最简单且最容易理解的素性测试的方法是试除法, 它用所有小于 a 的正整数去试除 a, 如果找到一个数能够整除 a, 那么这个数就是 a 的因数.

最简单且最容易理解的素性测试的方法是试除法, 它用所有小于 a 的正整数去试除 a, 如果找到一个数能够整除 a, 那么这个数就是 a 的因数.

试除法一定能够找到 a 的因数. 因为它检查 a 的所有可能的因数, 所以如果这个算法 “失败”, 也就证明了 a 是个素数.

最简单且最容易理解的素性测试的方法是试除法, 它用所有小于 a 的正整数去试除 a, 如果找到一个数能够整除 a, 那么这个数就是 a 的因数.

试除法一定能够找到 a 的因数. 因为它检查 a 的所有可能的因数, 所以如果这个算法 "失败", 也就证明了 a 是个素数.

试除法中我们只需用小于 $\sqrt{a}$ 的素数去试除 a 即可:

定理 6.1. 如果 a 是合数, q 是它的除 1 以外的最小正因数, 则 $q \leq \sqrt{a}$.

最简单且最容易理解的素性测试的方法是试除法, 它用所有小于 a 的正整数去试除 a, 如果找到一个数能够整除 a, 那么这个数就是 a 的因数.

试除法一定能够找到 a 的因数. 因为它检查 a 的所有可能的因数, 所以如果这个算法 "失败", 也就证明了 a 是个素数.

试除法中我们只需用小于 $\sqrt{a}$ 的素数去试除 a 即可:

定理 6.1. 如果 a 是合数, q 是它的除 1 以外的最小正因数, 则 $q \leq \sqrt{a}$.

证明: 因为 a 是合数, q 是它的一个因数, 所以存在 $b \in \mathbb{Z}$ 使得 $a = bq$. 又因为 q 是 a 的最小正因数, 所以 $b \geq q$, 于是 $a \geq q^2$, 即 $q \leq \sqrt{a}$. □

显然, 对任意合数, 它除 1 以外的最小正因数必为素数, 因此由上面的定理我们有下述推论.

推论 6.1. 设 $a \in \mathbb{Z}$, $a > 1$, 则 a 是素数的充要条件是对任意素数 p $(1 < p \leq \sqrt{a})$, 都有 $p \nmid a$.

显然, 对任意合数, 它除 1 以外的最小正因数必为素数, 因此由上面的定理我们有下述推论.

推论 6.1. 设 $a \in \mathbb{Z}$, $a > 1$, 则 a 是素数的充要条件是对任意素数 p $(1 < p \leq \sqrt{a})$, 都有 $p \nmid a$.

由推论6.1, 我们只需用 1 到 $\sqrt{a}$ 之间的每个素数去除 a 即可判断 a 是否是素数.

例如, 要判断 101 是否是素数, 我们只需用 $2, 3, 5, 7$ 去除 101 即可, 因为这些数均不整除 101, 所以 101 是素数.

公元前 250 年, 古希腊数学家厄拉多塞基于推论6.1发明了一种求出所有不大于数 a 的素数的方法, 后人称为**厄拉多塞筛法**.

公元前 250 年, 古希腊数学家厄拉多塞基于推论6.1发明了一种求出所有不大于数 a 的素数的方法, 后人称为**厄拉多塞筛法**.

其做法是这样的: 假定 a 是任意给定的正整数, 我们把 1 到 a 的正整数按照从小到大的顺序写出:

$$1, 2, 3, 4, 5, 6, 7, \ldots, a,$$

先把 1 划去; 剩下的第一个数是 2, 我们保留 2, 但划去 2 的所有其他倍数; 下一个剩下的数是 3, 我们保留 3, 划去 3 的所有其他倍数; 再下一个剩下的数是 5, 我们保留 5, 划去 5 的所有其他倍数; ...

我们继续这个过程直到 $\sqrt{a}$, 当把所有不大于 $\sqrt{a}$ 的素数的倍数划去后, 剩下的数就是所有不大于 a 的素数.

这是因为根据推论6.1, 划去的数都不是素数, 而所有剩下的数都没有小于它们自身的因数, 因此由推论6.1知这些数都是素数.

这是因为根据推论6.1, 划去的数都不是素数, 而所有剩下的数都没有小于它们自身的因数, 因此由推论6.1知这些数都是素数.

我们以 $a = 48$ 为例来看看如何用厄拉多塞筛法求出所有 48 以内的素数.

这时, 因为 $\sqrt{a} < 7$, 在下面的表中划去所有小于 7 的素数 (即 $2, 3, 5$) 的大于自身的倍数, 剩下的数 $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$ 就是所有不大于 48 的素数.

这是因为根据推论6.1, 划去的数都不是素数, 而所有剩下的数都没有小于它们自身的因数, 因此由推论6.1知这些数都是素数.

我们以 $a = 48$ 为例来看看如何用厄拉多塞筛法求出所有 48 以内的素数.

这时, 因为 $\sqrt{a} < 7$, 在下面的表中划去所有小于 7 的素数 (即 $2, 3, 5$) 的大于自身的倍数, 剩下的数 $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47$ 就是所有不大于 48 的素数.

~~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~~

下面介绍两种初等的整数分解方法, 它们仅仅对不太大的整数适用.

第一种是试除法. 假设我们想将 a 写成一些素数之积, 那么我们先用小于 $\sqrt{a}$ 的素数去试除 a, 直到找到一个素因数 p, 然后对 a/p $(< a)$ 做同样的事情, 直到发现 a 的所有因数.

下面介绍两种初等的整数分解方法, 它们仅仅对不太大的整数适用.

第一种是试除法. 假设我们想将 a 写成一些素数之积, 那么我们先用小于 $\sqrt{a}$ 的素数去试除 a, 直到找到一个素因数 p, 然后对 a/p $(< a)$ 做同样的事情, 直到发现 a 的所有因数.

例 6.1. 用试除法分解 $a = 9361$.

下面介绍两种初等的整数分解方法, 它们仅仅对不太大的整数适用.

第一种是试除法. 假设我们想将 a 写成一些素数之积, 那么我们先用小于 $\sqrt{a}$ 的素数去试除 a, 直到找到一个素因数 p, 然后对 a/p $(< a)$ 做同样的事情, 直到发现 a 的所有因数.

例 6.1. 用试除法分解 $a = 9361$.

解: $2, 3, 5, 7$ 均不整除 9361, 最小的整除 9361 的数是 11, 其商为 851, 即 $9361/11 = 851$. 因为 $\sqrt{851} \approx 29.17 > 11$, 所以我们暂时无法确定 851 是否是素数. 继续用不小于 11 的素数试除 851, 有 $23|851$, 其商为 37. 因为 $\sqrt{37} < 23$, 所以 37 必是素数. 于是 $9361 = 11 \cdot 23 \cdot 37$. □

在试除法中, 我们是不断地用更大的素数去除被分解数, 直到得到它的分解. 这种试除法一直没有被改进, 直到费马应用平方差公式 $m^2 - n^2 = (m + n)(m - n)$ 来分解因数.

在试除法中, 我们是不断地用更大的素数去除被分解数, 直到得到它的分解. 这种试除法一直没有被改进, 直到费马应用平方差公式 $m^2 - n^2 = (m + n)(m - n)$ 来分解因数.

费马分解法是对奇数考虑的, 在这种方法中, 从被分解数 a 开始, 找到不小于 a 的最小平方数 s^2, 检查 s^2 与 a 的差 $s^2 - a$ 是否是平方数.

在试除法中, 我们是不断地用更大的素数去除被分解数, 直到得到它的分解. 这种试除法一直没有被改进, 直到费马应用平方差公式 $m^2 - n^2 = (m + n)(m - n)$ 来分解因数.

费马分解法是对奇数考虑的, 在这种方法中, 从被分解数 a 开始, 找到不小于 a 的最小平方数 s^2, 检查 s^2 与 a 的差 $s^2 - a$ 是否是平方数.

如果是, 假设 $s^2 - a = t^2$, 那么就可以利用平方差分解的技巧来分解 a, 即 $a = (s + t)(s - t)$;

在试除法中, 我们是不断地用更大的素数去除被分解数, 直到得到它的分解. 这种试除法一直没有被改进, 直到费马应用平方差公式 $m^2 - n^2 = (m + n)(m - n)$ 来分解因数.

费马分解法是对奇数考虑的, 在这种方法中, 从被分解数 a 开始, 找到不小于 a 的最小平方数 s^2, 检查 s^2 与 a 的差 $s^2 - a$ 是否是平方数.

如果是, 假设 $s^2 - a = t^2$, 那么就可以利用平方差分解的技巧来分解 a, 即 $a = (s + t)(s - t)$;

如果不是, 那么找下一个平方数 $(s + 1)^2$, 重复上面的处理. 该过程一定终止, 因为至少 $(\frac{a+1}{2})^2$ 可以满足条件, 即 $(\frac{a+1}{2})^2 - a = (\frac{a-1}{2})^2$, 此时给出平凡分解 $a = a \cdot 1$.

如果该过程直到 $(\frac{a+1}{2})^2$ 才终止 (即对任意整数
$s \in [\sqrt{a}, \frac{a+1}{2})$, $s^2 - a$ 都不是平方数), 那么易证 a 必是素数.

如果该过程直到 $(\frac{a+1}{2})^2$ 才终止 (即对任意整数
$s \in [\sqrt{a}, \frac{a+1}{2})$, $s^2 - a$ 都不是平方数), 那么易证 a 必是素数.

事实上, 假设 a 不是素数, 有分解 $a = mn$ $(1 < m, n < a)$,
则有 $a = (\frac{m+n}{2})^2 - (\frac{m-n}{2})^2$. 令 $s = \frac{m+n}{2}$, 则有 $s \geq \sqrt{a}$,
$s < \frac{mn+1}{2} = \frac{a+1}{2}$, 且 $s^2 - a = (\frac{m-n}{2})^2$ 是平方数, 矛盾!

例 6.2. 用费马分解法分解 $a = 145$.

例 6.2. 用费马分解法分解 $a = 145$.

解: 第一个大于 145 的平方数是 $169 = 13^2$. 下面按照费马分解法的步骤计算平方数 s^2 及 $s^2 - a$:

$$\begin{aligned} 13^2 - 145 &= 24 \\ 14^2 - 145 &= 51 \\ 15^2 - 145 &= 80 \\ 16^2 - 145 &= 111 \\ 17^2 - 145 &= 144 = 12^2. \end{aligned}$$

因此, $145 = 17^2 - 12^2 = 5 \cdot 29$. □

例 6.2. 用费马分解法分解 $a = 145$.

解: 第一个大于 145 的平方数是 $169 = 13^2$. 下面按照费马分解法的步骤计算平方数 s^2 及 $s^2 - a$:

$$\begin{aligned} 13^2 - 145 &= 24 \\ 14^2 - 145 &= 51 \\ 15^2 - 145 &= 80 \\ 16^2 - 145 &= 111 \\ 17^2 - 145 &= 144 = 12^2. \end{aligned}$$

因此, $145 = 17^2 - 12^2 = 5 \cdot 29$. □

费马分解法有时是非常低效的, 因为使用这种方法, 有时必须检查 $\frac{a+1}{2} - \lfloor\sqrt{a}\rfloor$ 个数是否是平方数 (这里 $\lfloor x\rfloor$ 是下取整函数, 即表示不超过 x 的整数中最大的一个).

1. 整除
2. 最大公因数与欧几里得算法
3. 最小公倍数
4. 一次不定方程
5. 算术基本定理
6. 厄拉多塞筛法
7. **素数分布**

下面的定理及其优美的证明最早出现在 2000 多年前欧几里得的《几何原本》中.

定理 7.1. 素数有无穷多个.

下面的定理及其优美的证明最早出现在 2000 多年前欧几里得的《 几何原本 》中.

定理 7.1. 素数有无穷多个.

证明: 假设只有有限多个素数, 设为 $p_1, p_2, \ldots, p_k$. 令 $p = p_1 p_2 \cdots p_k + 1$. 由命题5.1, 存在素数 $p' | p$. 显然, $p' \notin \{p_1, p_2, \ldots, p_k\}$, 否则 $p' | p_1 p_2 \cdots p_k$, 从而导致 $p' | 1$, 矛盾! 因此, p' 是个不同于 $p_1, p_2, \ldots, p_k$ 的素数, 但这与 $p_1, p_2, \ldots, p_k$ 是所有素数的假设矛盾, 故素数有无穷多个. □

素数不但有无穷多个, 而且具有某些特殊形式的素数往往也有无穷多个, 下面就是一个例子.

定理 7.2. 存在无穷多个形如 $4n-1$ 的素数.

素数不但有无穷多个, 而且具有某些特殊形式的素数往往也有无穷多个, 下面就是一个例子.

定理 7.2. 存在无穷多个形如 $4n-1$ 的素数.

证明: 假设形如 $4n-1$ 的素数只有有限多个, 它们中最大的一个记为 p. 令 $a=4p'-1$, 其中 p' 是所有不超过 p 的奇素数之积. 显然, $a>p$. 又因为 a 是 $4n-1$ 形的, 所以 a 必为合数. 如果素数 $p''|a$, 则易见 $p''>p$, 否则 $p''|p'$, 这将导致 $p''|1$, 矛盾! 因为 a 是奇数, 所以 p'' 只能是形如 $4n+1$ 或 $4n-1$ 的. 由于两个 $4n+1$ 形数的乘积仍为 $4n+1$ 形, 故 a 的素因数中必有一个是 $4n-1$ 形的, 即存在大于 p 的 $4n-1$ 形的素数, 矛盾! 因此定理成立. □

一般地, 我们有下面的定理, 它最早由德国数学家狄利克雷于 1837 年用复分析的方法证明.

定理 7.3. 设正整数 k, l 满足 $(k, l) = 1$, 则形如 $kn + l$ 的素数有无穷多个.

一般地, 我们有下面的定理, 它最早由德国数学家狄利克雷于 1837 年用复分析的方法证明.

定理 7.3. 设正整数 k, l 满足 $(k, l) = 1$, 则形如 $kn + l$ 的素数有无穷多个.

下面的定理告诉我们, 两个相邻素数之间可能间隔任意多个合数, 这表明素数的分布是极不规则的.

定理 7.4. 对任意正整数 k, 存在 k 个连续的合数.

一般地, 我们有下面的定理, 它最早由德国数学家狄利克雷于 1837 年用复分析的方法证明.

定理 7.3. 设正整数 k, l 满足 $(k, l) = 1$, 则形如 $kn + l$ 的素数有无穷多个.

下面的定理告诉我们, 两个相邻素数之间可能间隔任意多个合数, 这表明素数的分布是极不规则的.

定理 7.4. 对任意正整数 k, 存在 k 个连续的合数.

证明: 对于给定的 k, 考虑下列 k 个连续的正整数:

$$(k+1)! + 2, (k+1)! + 3, \ldots, (k+1)! + (k+1).$$

因为 2 整除上面数列的第一个数, 3 整除第二个数, ..., $k+1$ 整除第 k 个数, 所以该数列中的 k 个数都是合数, 于是定理成立.

为了介绍著名的素数定理, 我们需要定义一个函数. 设 x 是任意实数, 定义 $\pi(x)$ 为不大于实数 x 的素数的个数.

例如, 当 $x < 2$ 时, $\pi(x) = 0$; $\pi(5) = \pi(5.7) = 3$.

为了介绍著名的素数定理, 我们需要定义一个函数. 设 x 是任意实数, 定义 $\pi(x)$ 为不大于实数 x 的素数的个数.

例如, 当 $x < 2$ 时, $\pi(x) = 0$; $\pi(5) = \pi(5.7) = 3$.

定理 7.5 (素数定理). 设 $x \in \mathbb{R}$, 则

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

为了介绍著名的素数定理, 我们需要定义一个函数. 设 x 是任意实数, 定义 $\pi(x)$ 为不大于实数 x 的素数的个数.

例如, 当 $x < 2$ 时, $\pi(x) = 0$; $\pi(5) = \pi(5.7) = 3$.

定理 7.5 (素数定理). 设 $x \in \mathbb{R}$, 则

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

素数定理表明, 当 x 趋近于正无穷大时, $\pi(x)$ 与 $x/\ln x$ 的比值趋近于 1, 这种趋势体现在下面的表中.

x	$\pi(x)$	$x/\ln x$	$\frac{\pi(x)}{x/\ln x}$
10^3	168	144.8	1.160
10^4	1229	1085.7	1.132
10^5	9592	8685.9	1.104
10^6	78498	72382.4	1.085
10^7	664579	620420.7	1.071
10^8	5761455	5428681.0	1.061
10^9	50847534	48254942.4	1.054
10^{10}	455052512	434294481.9	1.048
10^{11}	4118054813	3948131663.7	1.043
10^{12}	37607912018	36191206825.3	1.039
10^{13}	346065536839	334072678387.1	1.036
10^{14}	3204941750802	3102103442166.0	1.033

素数定理不仅仅是关于素数个数的一个理论结果, 它在数学和计算科学中也有很大的应用价值. 例如,

(1) 可以估计, 随机选取的一个整数 a 是素数的概率是 $1/\ln a$. 例如, 一个不超过 10^{1000} 的数是素数的概率大约是 $1/\ln 10^{1000} \approx 1/2302$.

素数定理不仅仅是关于素数个数的一个理论结果, 它在数学和计算科学中也有很大的应用价值. 例如,

(1) 可以估计, 随机选取的一个整数 a 是素数的概率是 $1/\ln a$. 例如, 一个不超过 10^{1000} 的数是素数的概率大约是 $1/\ln 10^{1000} \approx 1/2302$.

(2) 估计利用试除法进行素性测试时需要的计算步骤. 在测试 a 是否是素数时, 试除法中最多需要试除 $\pi(\sqrt{a})$ 个素数. 对于充分大的 a, 我们有 $\pi(\sqrt{a}) \approx \frac{\sqrt{a}}{\ln \sqrt{a}} = \frac{2\sqrt{a}}{\ln a}$. 如果小于 $\sqrt{a}$ 的素数表是已知的, 如果一台计算机执行一次除法需要 $\frac{\ln a}{10^6}$ 秒, 那么这台计算机检查 a 是素数需要大约 $\frac{2\sqrt{a}}{\ln a} \cdot \frac{\ln a}{10^6} = \frac{2\sqrt{a}}{10^6}$ 秒. 直接使用这种方法验证一个 30 位的素数将需要 63 年多时间.

最后, 我们简单提及有关素数的几个尚未解决的著名猜想.

最后, 我们简单提及有关素数的几个尚未解决的著名猜想.

哥德巴赫猜想. 每个大于 2 的偶数均能写成两个素数之和.

该猜想是哥德巴赫在 1742 年给欧拉的一封信中提出的. 这方面目前最好的结果是陈景润在 1966 年证明的: 所有充分大的整数都能表成一个素数和至多两个素数乘积之和.

最后, 我们简单提及有关素数的几个尚未解决的著名猜想.

哥德巴赫猜想. 每个大于 2 的偶数均能写成两个素数之和.

该猜想是哥德巴赫在 1742 年给欧拉的一封信中提出的. 这方面目前最好的结果是陈景润在 1966 年证明的: 所有充分大的整数都能表成一个素数和至多两个素数乘积之和.

孪生素数猜想. 存在无穷多个素数对 p 和 $p+2$.

关于孪生素数猜想, 1966 年陈景润证明了存在无穷多个素数 p 使得 $p+2$ 至多有两个素因数.

最后, 我们简单提及有关素数的几个尚未解决的著名猜想.

哥德巴赫猜想. 每个大于 2 的偶数均能写成两个素数之和.

该猜想是哥德巴赫在 1742 年给欧拉的一封信中提出的. 这方面目前最好的结果是陈景润在 1966 年证明的: 所有充分大的整数都能表成一个素数和至多两个素数乘积之和.

孪生素数猜想. 存在无穷多个素数对 p 和 $p+2$.

关于孪生素数猜想, 1966 年陈景润证明了存在无穷多个素数 p 使得 $p+2$ 至多有两个素因数.

n^2+1 猜想. 存在无穷多个形如 n^2+1 的素数, 这里 n 是正整数.

目前有关 n^2+1 猜想的最好的结果是 1973 年 Henryk Iwaniec 得到的: 存在无穷多个整数 n 使得 n^2+1 或者是素数或者是两个素数之积.