网络空间安全学院

School of Cyberspace Security, BUPT

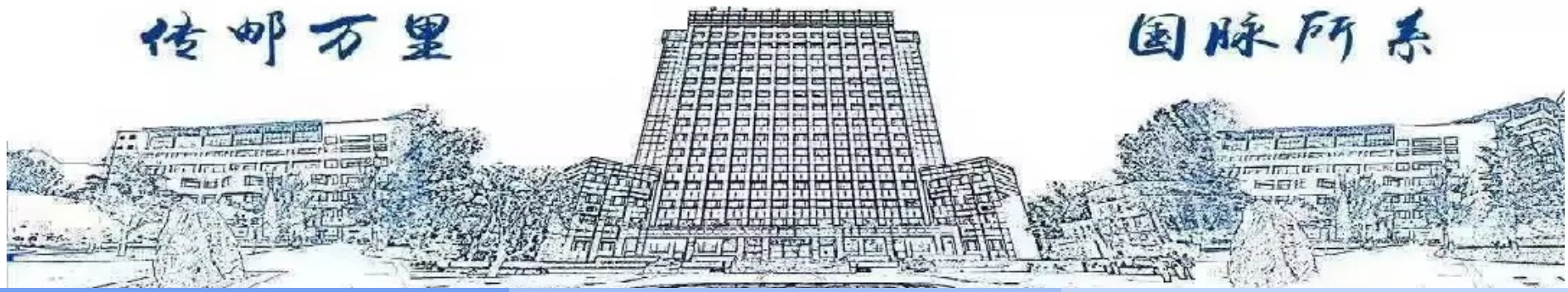
信息安全数学基础

—— 整数的可除性 (2)

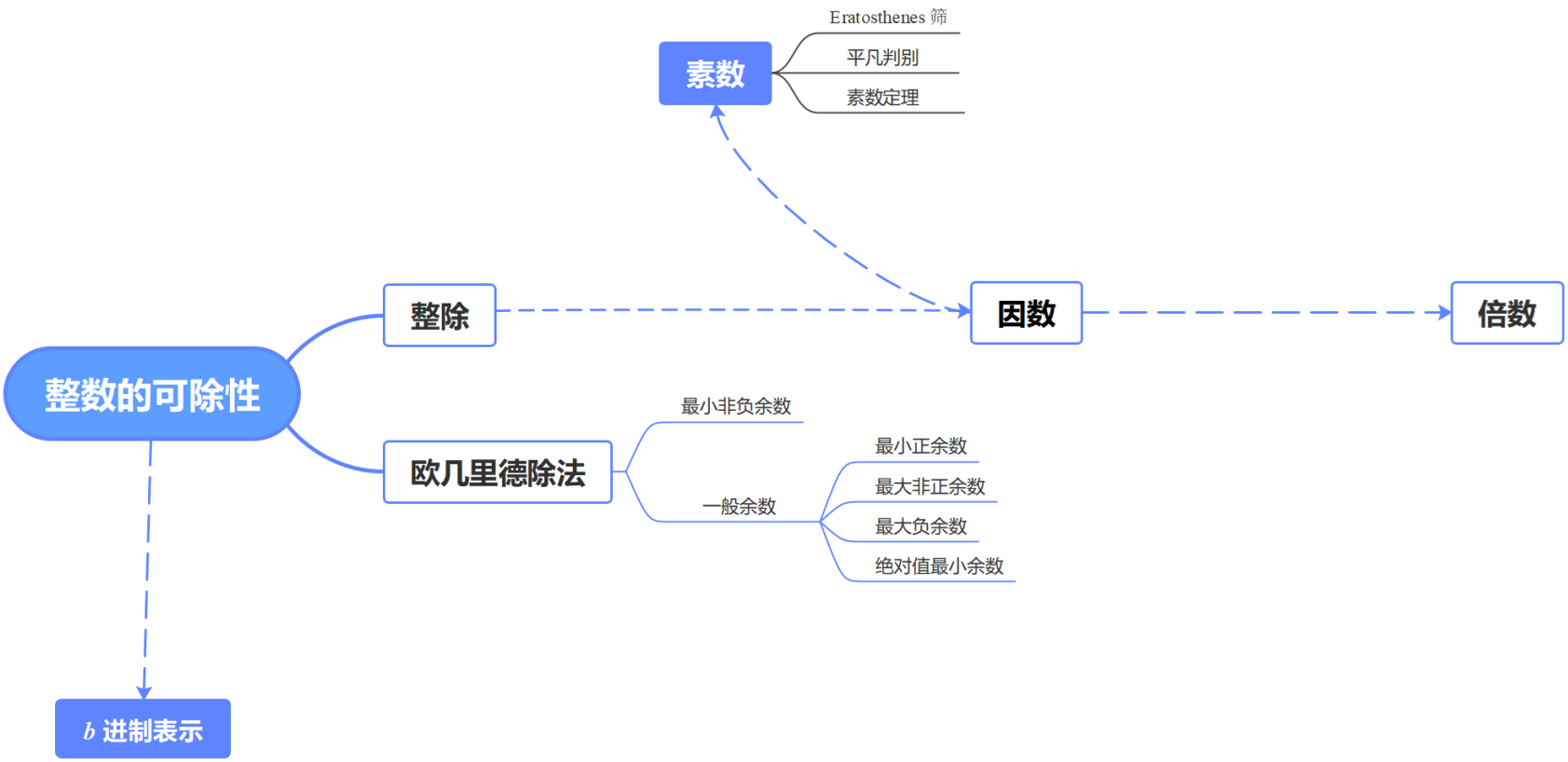
信数课题组

北京邮电大学网络空间安全学院

2024 年 9 月 17 日



上次课回顾


整数的可除性
整除
因数
倍数
素数
Eratosthenes 筛
平凡判别
素数定理
欧几里德除法
最小非负余数
一般余数
最小正余数
最大非正余数
最大负余数
绝对值最小余数
b 进制表示

目录

目录

从单个整数的因数, 考虑多个整数的公共因数（简称公因数）, 特别是最大的公因数及其计算.

定义 1.2.1

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

从单个整数的因数, 考虑多个整数的公共因数（简称公因数）, 特别是最大的公因数及其计算.

定义 1.2.1

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

定义 1.2.2

设 d 是 $a_1, \cdots, a_n$ 的一个公因数的数学表达式为

$$d \mid a_1, \cdots, d \mid a_n.$$

如果整数 $a_1, \cdots, a_n$ 不全为零, 那么 $a_1, \cdots, a_n$ 的所有公因数中最大的一个公因数叫做 $a_1, \cdots, a_n$ 的**最大公因数**, 记作 $(a_1, \cdots, a_n)$.

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

定理 1.2.1

设 $a_1, \cdots, a_n$ 是 n 个不全为零的整数, 则

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

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

定理 1.2.1

设 $a_1, \cdots, a_n$ 是 n 个不全为零的整数, 则

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

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

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

定理 1.2.1

设 $a_1, \cdots, a_n$ 是 n 个不全为零的整数, 则

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

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

证: (i) 设 $d \mid a_i, 1 \leqslant i \leqslant n$, 有 $d \mid |a_i|, 1 \leqslant i \leqslant n$, 故 $a_1, \cdots, a_n$ 的公因数也是 $|a_1|, \cdots, |a_n|$ 的公因数. 反之, 设 $d \mid |a_i|, 1 \leqslant i \leqslant n$, 同样有 $d \mid a_i, 1 \leqslant i \leqslant n$, 故 $|a_1|, \cdots, |a_n|$ 的公因数也是 $a_1, \cdots, a_n$ 的公因数.

定理 1.2.1

设 $a_1, \cdots, a_n$ 是 n 个不全为零的整数, 则

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

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

证： (i) 设 $d \mid a_i, 1 \leqslant i \leqslant n$, 有 $d \mid |a_i|, 1 \leqslant i \leqslant n$, 故 $a_1, \cdots, a_n$ 的公因数也是 $|a_1|, \cdots, |a_n|$ 的公因数. 反之, 设 $d \mid |a_i|, 1 \leqslant i \leqslant n$, 同样有 $d \mid a_i, 1 \leqslant i \leqslant n$, 故 $|a_1|, \cdots, |a_n|$ 的公因数也是 $a_1, \cdots, a_n$ 的公因数. 故, $a_1, \cdots, a_n$ 与 $|a_1|, \cdots, |a_n|$ 的公因数相同.

定理 1.2.1

设 $a_1, \cdots, a_n$ 是 n 个不全为零的整数, 则

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

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

证: (i) 设 $d \mid a_i, 1 \leqslant i \leqslant n$, 有 $d \mid |a_i|, 1 \leqslant i \leqslant n$, 故 $a_1, \cdots, a_n$ 的公因数也是 $|a_1|, \cdots, |a_n|$ 的公因数. 反之, 设 $d \mid |a_i|, 1 \leqslant i \leqslant n$, 同样有 $d \mid a_i, 1 \leqslant i \leqslant n$, 故 $|a_1|, \cdots, |a_n|$ 的公因数也是 $a_1, \cdots, a_n$ 的公因数. 故, $a_1, \cdots, a_n$ 与 $|a_1|, \cdots, |a_n|$ 的公因数相同.

(ii) 由 (i) 立得 (ii).

定理 1.2.1

设 $a_1, \cdots, a_n$ 是 n 个不全为零的整数, 则

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

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

证： (i) 设 $d \mid a_i, 1 \leqslant i \leqslant n$, 有 $d \mid |a_i|, 1 \leqslant i \leqslant n$, 故 $a_1, \cdots, a_n$ 的公因数也是 $|a_1|, \cdots, |a_n|$ 的公因数. 反之, 设 $d \mid |a_i|, 1 \leqslant i \leqslant n$, 同样有 $d \mid a_i, 1 \leqslant i \leqslant n$, 故 $|a_1|, \cdots, |a_n|$ 的公因数也是 $a_1, \cdots, a_n$ 的公因数. 故, $a_1, \cdots, a_n$ 与 $|a_1|, \cdots, |a_n|$ 的公因数相同.

(ii) 由 (i) 立得 (ii).

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

定理 1.2.1

设 $a_1, \cdots, a_n$ 是 n 个不全为零的整数, 则

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

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

证: (i) 设 $d \mid a_i, 1 \leqslant i \leqslant n$, 有 $d \mid |a_i|, 1 \leqslant i \leqslant n$, 故 $a_1, \cdots, a_n$ 的公因数也是 $|a_1|, \cdots, |a_n|$ 的公因数. 反之, 设 $d \mid |a_i|, 1 \leqslant i \leqslant n$, 同样有 $d \mid a_i, 1 \leqslant i \leqslant n$, 故 $|a_1|, \cdots, |a_n|$ 的公因数也是 $a_1, \cdots, a_n$ 的公因数. 故, $a_1, \cdots, a_n$ 与 $|a_1|, \cdots, |a_n|$ 的公因数相同.

(ii) 由 (i) 立得 (ii).

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

例 1.2.2 三个整数 $6, 25$ 和 35 的公因数为 $\{\pm 1\}$, $(6, 25, 35) = 1$. 或者说, $6, 25$ 和 35 是互素的.

例 1.2.3　设 a, b 是两个正整数, 如果 $b \mid a$, 则 $(a, b) = b$.

例 1.2.3　设 a, b 是两个正整数, 如果 $b \mid a$, 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 1.2.3　设 a, b 是两个正整数, 如果 $b \mid a$, 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 a 与 p 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 1.2.3　设 a, b 是两个正整数, 如果 $b \mid a$, 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 a 与 p 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, 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

$$a = q \cdot b + c,$$

其中 q 是整数, 则 $(a, b) = (b, c)$.

定理 1.2.2

设 a, b, c 是三个不全为零的整数. 如果

$$a = q \cdot b + c,$$

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 得, $d \mid a + (-q) \cdot b$. 而 $a + (-q) \cdot b = c$, 故 d 是 b, c 的公因数. 从而, $d \leqslant d'$.

同理, 由 $d' \mid b, d' \mid c$ 得, $d' \mid q \cdot b + c$. 而 $q \cdot b + c = a$, 故 d' 是 a, b 的公因数. 从而, $d' \leqslant d$.

因此, $d = d'$, 即证 $(a, b) = (b, c)$.

定理 1.2.2

设 a, b, c 是三个不全为零的整数. 如果

$$a = q \cdot b + c,$$

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 得, $d \mid a + (-q) \cdot b$. 而 $a + (-q) \cdot b = c$, 故 d 是 b, c 的公因数. 从而, $d \leqslant d'$.

同理, 由 $d' \mid b, d' \mid c$ 得, $d' \mid q \cdot b + c$. 而 $q \cdot b + c = a$, 故 d' 是 a, b 的公因数. 从而, $d' \leqslant d$.

因此, $d = d'$, 即证 $(a, b) = (b, c)$.

例 1.2.7　因为 $2409 = 6 \cdot 365 + 219$, 所以有 $(202409, 365) = (365, 219)$. 因为 $365 = 1 \cdot 219 + 146$, 所以有 $(365, 219) = (219, 146) = 73$.

目录

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 $r_{-2} = a, r_{-1} = b$. 反复运用欧几里德除法, 有

$$\begin{aligned}
r_{-2} &= q_0 \cdot r_{-1} + r_0, \quad 0 < r_0 < r_{-1}, \\
r_{-1} &= q_1 \cdot r_0 + r_1, \quad 0 < r_1 < r_0, \\
&\vdots \\
r_{n-2} &= q_n \cdot r_{n-1} + r_n, \quad 0 < r_n < r_{n-1}, \\
r_{n-1} &= q_{n+1} \cdot r_n + r_{n+1}, \quad r_{n+1} = 0.
\end{aligned} \tag{1.2.1}$$

经过有限步骤, 必然存在 n 使得 $r_{n+1} = 0$, 这是因为

$$0 = r_{n+1} < r_n < r_{n-1} < \cdots < r_1 < r_0 < r_{-1} = b, \text{且 } b \text{ 是有限正整数.}$$

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式 (1.2.1) 中最后一个非零余数.

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式 (1.2.1) 中最后一个非零余数.

证：根据定理 1.2.2，有

$$\begin{aligned}(a, b) &= (b, r_0)\\ &= (r_0, r_1)\\ &= \cdots\\ &= (r_{n-1}, r_n)\\ &= (r_n, 0)\end{aligned}$$

所以有 $(a, b) = (r_n, 0) = r_n$. 因此, 结论成立.

广义欧几里德除法 (辗转相除法)

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.
其具体过程详述如下:

(1) 根据定理 1.2.1, 将求两个整数的最大公因数转化成求两个非负整数的最大公因数;

(2) 运用欧几里德除法, 并根据定理 1.2.3, 可以将求两个正整数的最大公因数转化成求两个较小非负整数的最大公因数;

(3) 反复运用欧几里德除法, 即广义欧几里德除法, 将求两个正整数的最大公因数转化成求 0 和一个正整数的最大公因数.

(4) 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).

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

$$377 = 1 \cdot 221 + 156,$$

$$221 = 1 \cdot 156 + 65,$$

$$156 = 2 \cdot 65 + 26,$$

$$65 = 2 \cdot 26 + 13,$$

$$26 = 2 \cdot 13 + 0.$$

所以, $(377, 221) = 13$.

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

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

解：方法一：利用广义欧几里德除法 (最小非负余数).

$$
\begin{aligned}
518860799 &= 2 \cdot 259339331 + 182137, \\
259339331 &= 1423 \cdot 182137 + 158380, \\
182137 &= 1 \cdot 158380 + 23757, \\
158380 &= 6 \cdot 23757 + 15838, \\
23757 &= 1 \cdot 15838 + 7919, \\
15838 &= 2 \cdot 7919.
\end{aligned}
$$

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

解：方法一：利用广义欧几里德除法 (最小非负余数).

$$\begin{aligned}
518860799 &= 2 \cdot 259339331 + 182137,\\
259339331 &= 1423 \cdot 182137 + 158380,\\
182137 &= 1 \cdot 158380 + 23757,\\
158380 &= 6 \cdot 23757 + 15838,\\
23757 &= 1 \cdot 15838 + 7919,\\
15838 &= 2 \cdot 7919.
\end{aligned}$$

方法二：利用广义欧几里德除法 (绝对值最小余数).

$$\begin{aligned}
518860799 &= 2 \cdot 259339331 + 182137,\\
259339331 &= 1424 \cdot 182137 - 23757,\\
182137 &= 8 \cdot 23757 - 7919,\\
23757 &= 3 \cdot 7919.
\end{aligned}$$

所以, $(518860799, 259339331) = 7919$.

目录

从广义欧几里德除法的算式 (1.2.1) 中, 可观察到

$$\begin{aligned} r_n &= (-q_n)\cdot r_{n-1} \quad + r_{n-2}, \\ r_{n-1} &= (-q_{n-1})\cdot r_{n-2} + r_{n-3}, \\ &\vdots \\ r_0 &= (-q_0)\cdot r_{-1} \quad + r_{-2}. \end{aligned}$$

从广义欧几里德除法的算式 (1.2.1) 中, 可观察到

$$\begin{aligned} r_n &= (-q_n)\cdot r_{n-1} \quad + r_{n-2}, \\ r_{n-1} &= (-q_{n-1})\cdot r_{n-2} + r_{n-3}, \\ &\vdots \\ r_0 &= (-q_0)\cdot r_{-1} \quad + r_{-2}. \end{aligned}$$

逐次消去 $r_{n-1}, \cdots, r_1, r_0$, 可找到整数 s, t 使得 $s\cdot a + t\cdot b = (a, b)$.

从广义欧几里德除法的算式 (1.2.1) 中, 可观察到

$$\begin{aligned} r_n &= (-q_n)\cdot r_{n-1} \quad + r_{n-2}, \\ r_{n-1} &= (-q_{n-1})\cdot r_{n-2} + r_{n-3}, \\ &\vdots \\ r_0 &= (-q_0)\cdot r_{-1} \quad + r_{-2}. \end{aligned}$$

逐次消去 $r_{n-1}, \cdots, r_1, r_0$, 可找到整数 s, t 使得 $s\cdot a + t\cdot b = (a, b)$.

定理 1.2.4

设 a, b 是任意两个正整数, 则存在整数 s, t 使得

$$s\cdot a + t\cdot b = (a, b).$$

成立, 该式叫做 **贝祖 (Bézout) 等式**.

例 1.2.10　设 $a = 377, b = 221$, 求整数 s, t, 使得

$$s \cdot a + t \cdot b = (a, b).$$

例 1.2.10　设 $a = 377, b = 221$, 求整数 s, t, 使得

$$s \cdot a + t \cdot b = (a, b).$$

解：由例 1.2.8 有

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

$$377 = 1 \cdot 221 + 156,$$

$$221 = 1 \cdot 156 + 65,$$

$$156 = 2 \cdot 65 + 26,$$

$$65 = 2 \cdot 26 + 13,$$

$$26 = 2 \cdot 13 + 0.$$

所以, $(377, 221) = 13$.

例 1.2.10　设 $a = 377, b = 221$, 求整数 s, t, 使得

$$s \cdot a + t \cdot b = (a, b).$$

解：由例 1.2.8 有

$$\begin{aligned}
13 &= (-2) \cdot 26 &&+ 65 \\
&\overset{\text{替代}}{=} \underbrace{(-2) \cdot (}_{\triangle\ \text{同类合并}}\underbrace{(-2) \cdot 65 + 156}_{\blacktriangle\ \text{拆分}}\underbrace{)}_{\triangle\ \text{同类合并}} &&+ \underbrace{65}_{\triangle} \\
&= \underbrace{5}_{\triangle} \cdot \underbrace{((-1) \cdot 156 + 221)}_{\text{类似地, 替代 } 65} &&+ \underbrace{(-2) \cdot 156}_{\blacktriangle} \\
&= \underbrace{(\ -7\ )}_{\triangle\ \text{同类合并}} \cdot \underbrace{((-1) \cdot 221 + 337)}_{\text{类似地, 替代 } 156} + \underbrace{5 \cdot 221}_{\text{拆分}} \\
&= 12 \cdot 221 &&+ (-7) \cdot 337
\end{aligned}$$

例 1.2.10　设 $a = 377, b = 221$, 求整数 s, t, 使得

$$s \cdot a + t \cdot b = (a, b).$$

解：由例 1.2.8 有

$$\begin{aligned}
13 &= (-2) \cdot 26 &&+ 65 \\
&\overset{\text{替代}}{=} \underbrace{(-2) \cdot (}_{\triangle\ \text{同类合并}}\underbrace{(-2) \cdot 65 + 156}_{\blacktriangle\ \text{拆分}}\underbrace{)}_{\triangle\ \text{同类合并}} &&+ \underbrace{65}_{\triangle} \\
&= \underbrace{5}_{\triangle} \cdot \underbrace{((-1) \cdot 156 + 221)}_{\text{类似地, 替代 } 65} &&+ \underbrace{(-2) \cdot 156}_{\blacktriangle} \\
&= \underbrace{(\quad -7 \quad)}_{\triangle\ \text{同类合并}} \cdot \underbrace{((-1) \cdot 221 + 337)}_{\text{类似地, 替代 } 156} + \underbrace{5 \cdot 221}_{\text{拆分}} \\
&= 12 \cdot 221 &&+ (-7) \cdot 337
\end{aligned}$$

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

例 1.2.11　设 $a = 518860799, b = 259339331$, 求整数 s, t, 使得

$$s \cdot a + t \cdot b = (a, b).$$

例 1.2.11　设 $a = 518860799, b = 259339331$, 求整数 s, t, 使得

$$s \cdot a + t \cdot b = (a, b).$$

解：由例 1.2.9, 根据绝对值最小余数, 我们有

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

解：方法一：利用广义欧几里德除法 (最小非负余数).

$$\begin{aligned}
518860799 &= 2 \cdot 259339331 + 182137,\\
259339331 &= 1423 \cdot 182137 + 158380,\\
182137 &= 1 \cdot 158380 + 23757,\\
158380 &= 6 \cdot 23757 + 15838,\\
23757 &= 1 \cdot 15838 + 7919,\\
15838 &= 2 \cdot 7919.
\end{aligned}$$

方法二：利用广义欧几里德除法 (绝对值最小余数).

$$\begin{aligned}
518860799 &= 2 \cdot 259339331 + 182137,\\
259339331 &= 1424 \cdot 182137 - 23757,\\
182137 &= 8 \cdot 23757 - 7919,\\
23757 &= 3 \cdot 7919.
\end{aligned}$$

所以, $(518860799, 259339331) = 7919$.

例 1.2.11　设 $a = 518860799, b = 259339331$, 求整数 s, t, 使得

$$s \cdot a + t \cdot b = (a, b).$$

解：由例 1.2.9, 根据绝对值最小余数, 我们有

$$\begin{aligned}
7919 &= 8 \cdot 23757 + (-182137) \\
&\overset{\text{替代}}{=} \underbrace{8 \cdot (1424 \cdot 182137}_{\triangle\ \text{同类合并}} + \underbrace{(-259339331))}_{\blacktriangle\ \text{拆分}} + \underbrace{(-182137)}_{\triangle} \\
&= \underbrace{11391}_{\triangle} \cdot \underbrace{((-2) \cdot 259339331 + 518860799)}_{\text{类似地, 替代 } 182137} + \underbrace{(-8) \cdot 259339331}_{\blacktriangle} \\
&= (-22790) \cdot 221 + 11397 \cdot 518860799
\end{aligned}$$

例 1.2.11　设 $a = 518860799, b = 259339331$, 求整数 s, t, 使得

$$s \cdot a + t \cdot b = (a, b).$$

解：由例 1.2.9, 根据绝对值最小余数, 我们有

$$\begin{aligned}
7919 &= 8 \cdot 23757 + (-182137) \\
&\overset{\text{替代}}{=} \underbrace{8 \cdot (1424 \cdot 182137}_{\triangle\ \text{同类合并}} + \underbrace{(-259339331))}_{\blacktriangle\ \text{拆分}} + \underbrace{(-182137)}_{\triangle} \\
&= \underbrace{11391}_{\triangle} \cdot \underbrace{((-2) \cdot 259339331 + 518860799)}_{\text{类似地, 替代 } 182137} + \underbrace{(-8) \cdot 259339331}_{\blacktriangle} \\
&= (-22790) \cdot 221 + 11397 \cdot 518860799
\end{aligned}$$

因此, 整数 $s = 11397, t = -22790$ 满足 $s \cdot a + t \cdot b = (a, b)$.

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 $sa + tb = 1$.

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 可立即得到命题的必要性.

反过来,

设 $d = (a, b)$, 则有 $d \mid a, d \mid b$.

根据假设, 存在整数 s, t 使得 $sa + tb = 1$, 则有 $d \mid sa + tb$, 即 $d \mid 1$.

因此, $d = 1$, 即整数 a, b 互素.

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 可立即得到命题的必要性.

反过来,

设 $d = (a, b)$, 则有 $d \mid a, d \mid b$.

根据假设, 存在整数 s, t 使得 $sa + tb = 1$, 则有 $d \mid sa + tb$, 即 $d \mid 1$.

因此, $d = 1$, 即整数 a, b 互素.

例 1.2.12　设 4 个整数 a, b, c, d 满足关系式 $ad - bc = 1$, 则

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

目录

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 的最大公因数的充分必要条件是:

(i) $d \mid a, d \mid b$;　　(ii) 若 $e \mid a, e \mid b$, 则 $e \mid d$.

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 的最大公因数的充分必要条件是:

(i) $d \mid a, d \mid b$;　　(ii) 若 $e \mid a, e \mid b$, 则 $e \mid d$.

证: 必要性. 若 d 是整数 a,b 的最大公因数, 则显然有 (i) 成立.

再由广义欧几里德除法 (定理 1.2.4) 知, 存在整数 s,t 使得 $sa+tb=d$. 因此, 当 $e \mid a, e \mid b$ 时, 有 $e \mid sa+tb$, 即 $e \mid d$. 故 (ii) 成立.

充分性. (i) 说明 d 是 a,b 的公因数, (ii) 说明 d 是 a,b 的公因数中的最大数 (因为 $e \mid d$ 时, 有 $|e| \leqslant d$). 因此, d 是整数 a,b 的最大公因数.

定理 1.2.7

设 a,b 是任意两个不全为零的整数,

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

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

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

定理 1.2.7

设 a, b 是任意两个不全为零的整数,

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

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

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

证: 设 $d = (a, b), d' = (m \cdot a, m \cdot b)$.

由广义欧几里德除法, 存在整数 s, t 使得 $sa + tb = d$.

两端同乘以 m, 得到 $s(m \cdot a) + t(m \cdot b) = m \cdot d$. 因此, $d' \mid m \cdot d$.

又显然有 $m \cdot d \mid m \cdot a, m \cdot d \mid m \cdot b$. 根据定理 1.2.6 (ii), 有 $m \cdot d \mid d'$.

故 $d' = m \cdot d$, 即 (i) 成立.

再根据 (i), 当 $d \mid a, d \mid b$ 时, 有

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

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

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

故 (ii) 成立.

再根据 (i), 当 $d \mid a, d \mid b$ 时, 有

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

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

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

故 (ii) 成立.

例 1.2.13　设 $a = 11 \cdot 202409, b = 23 \cdot 202409$, 计算 (a,b).

再根据 (i), 当 $d \mid a, d \mid b$ 时, 有

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

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

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

故 (ii) 成立.

例 1.2.13　设 $a = 11 \cdot 202409, b = 23 \cdot 202409$, 计算 (a,b).

解：因为 $(11,23) = (11, 23 - 11 \cdot 2) = (11,1) = 1$,

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

定理 1.2.8

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

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

定理 1.2.8

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

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

证：令 $d = (ab, c), d' = (b, c)$, 有 $d' \mid b, d' \mid c$, 进而 $d' \mid ab, d' \mid c$.

根据定理 1.2.6, 得到 $d' \mid d$.

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 $s \cdot a + t \cdot c = 1$. 两端同时乘以 b, 得到 $s \cdot (ab) + (tb) \cdot c = b$.

由于 d 是 ab 与 c 的最大公因数, 有 $d \mid ab, d \mid c$, 进而可得到 $d \mid s \cdot (ab) + (tb) \cdot c$, 即 $d \mid b$. 故而 d 是 b 与 c 的公因数.

由于 d' 是 b 与 c 的最大公因数, 同样根据定理 1.2.6, 得到 $d \mid d'$.

故 $d = d'$.

推论 1.2.1

设 $n-1(n \geq 3), a_1, \cdots, a_n, c$ 为整数. 如果 $(a_i, c) = 1, 1 \leqslant i \leqslant n$, 则

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

推论 1.2.1

设 $n-1(n\geq 3), a_1,\cdots,a_n,c$ 为整数. 如果 $(a_i,c)=1, 1\leqslant i\leqslant n$, 则

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

证：对 n 作数学归纳法.

$n=2$ 时, 由定理 1.2.8 易得.

推论 1.2.1

设 $n-1(n\geq 3), a_1,\cdots,a_n,c$ 为整数. 如果 $(a_i,c)=1, 1\leqslant i\leqslant n$, 则

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

证：对 n 作数学归纳法.

$n=2$ 时, 由定理 1.2.8 易得.

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

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

再根据 $(a_n,c)=1$ 及定理 1.2.8 得

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

因此, 命题对所有的 n 成立.

对于 n 个整数 $a_1, \cdots, a_n$, 可以用递归的方法, 将求它们的最大公因数转化成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

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

则 $(a_1, a_2, \cdots, a_n) = d_n$.

对于 n 个整数 $a_1, \cdots, a_n$, 可以用递归的方法, 将求它们的最大公因数转化成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

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

则 $(a_1, a_2, \cdots, a_n) = d_n$.

例 1.2.14　计算最大公因数 $(12, 25, 100, 256)$.

对于 n 个整数 $a_1, \cdots, a_n$, 可以用递归的方法, 将求它们的最大公因数转化成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

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

则 $(a_1, a_2, \cdots, a_n) = d_n$.

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

对于 n 个整数 $a_1, \cdots, a_n$, 可以用递归的方法, 将求它们的最大公因数转化成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

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

则 $(a_1, a_2, \cdots, a_n) = d_n$.

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, d 是正整数. 则 d 是整数 $a_1, \cdots, a_n$ 的最大公因数的充要条件是:

(i) $d \mid a_1, \cdots, d \mid a_n$;　　(ii) 若 $e \mid a_1, \cdots, e \mid a_n$, 则 $e \mid d$.

进一步讨论最大公因数与整除相关的性质.

定理 1.2.9

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

进一步讨论最大公因数与整除相关的性质.

定理 1.2.9

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

证：根据假设条件和定理 1.2.8, 有 $c \mid (ab, c)$, 且 $(ab, c) = (b, c)$, 则 $c \mid (b, c)$. 从而, $c \mid b$.

进一步讨论最大公因数与整除相关的性质.

定理 1.2.9

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

证：根据假设条件和定理 1.2.8, 有 $c \mid (ab, c)$, 且 $(ab, c) = (b, c)$, 则 $c \mid (b, c)$. 从而, $c \mid b$.

定理 1.2.10

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

进一步讨论最大公因数与整除相关的性质.

定理 1.2.9

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

证：根据假设条件和定理 1.2.8, 有 $c \mid (ab, c)$, 且 $(ab, c) = (b, c)$, 则 $c \mid (b, c)$. 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, 则有 $(a, p) = 1$.

再由 $p \mid ab$, 根据定理 1.2.9, 有 $p \mid b$. 从而结论成立.

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 $a_k, 1 \leqslant k \leqslant n$.

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 $a_k, 1 \leqslant k \leqslant n$.

证：若 $a_1, \cdots, a_n$ 都不能被 p 整除, 由已知 p 是素数, 有

$$(a_i, p) = 1, 1 \leqslant i \leqslant n.$$

进而, $(a_1 \cdots a_n, p) = 1$. 这与 $p \mid a_1 \cdots a_n$ 矛盾.

所以, 结论成立.

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 $a_k, 1 \leqslant k \leqslant n$.

证：若 $a_1, \cdots, a_n$ 都不能被 p 整除, 由已知 p 是素数, 有

$$(a_i, p) = 1, 1 \leqslant i \leqslant n.$$

进而, $(a_1 \cdots a_n, p) = 1$. 这与 $p \mid a_1 \cdots a_n$ 矛盾.

所以, 结论成立.

例 1.2.15　因为 $365 \mid 12 \cdot 2555$, 又 $(365, 12) = 1$, 所以 $365 \mid 2555$.

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 $a_k, 1 \leqslant k \leqslant n$.

证：若 $a_1, \cdots, a_n$ 都不能被 p 整除, 由已知 p 是素数, 有

$$(a_i, p) = 1, 1 \leqslant i \leqslant n.$$

进而, $(a_1 \cdots a_n, p) = 1$. 这与 $p \mid a_1 \cdots a_n$ 矛盾.

所以, 结论成立.

例 1.2.15 因为 $365 \mid 12 \cdot 2555$, 又 $(365, 12) = 1$, 所以 $365 \mid 2555$.

例 1.2.16 因为 $7 \mid 5 \cdot 2555$, 又 $7 \nmid 5$ 及 7 为素数, 所以 $7 \mid 2555$.

目录

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 $a_1, \cdots, a_n$ 的**最小公倍数**, 记作 $[a_1, \cdots, a_n]$.

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 $a_1, \cdots, a_n$ 的**最小公倍数**, 记作 $[a_1, \cdots, a_n]$.

定理 1.2.11

设 a, b 是两个互素的正整数, 则

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

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

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 $a_1, \cdots, a_n$ 的**最小公倍数**, 记作 $[a_1, \cdots, a_n]$.

定理 1.2.11

设 a, b 是两个互素的正整数, 则

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

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

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 $a_1, \cdots, a_n$ 的**最小公倍数**, 记作 $[a_1, \cdots, a_n]$.

定理 1.2.11

设 a, b 是两个互素的正整数, 则

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

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

证: (i) 设 $b \mid m$, 则存在整数 k 使得 $m = k \cdot b$. 又 $a \mid m$, 即 $a \mid k \cdot b$, 而 $(a, b) = 1$, 由定理 1.2.9 知, $a \mid k$, 则存在整数 t 使得 $k = t \cdot a$. 从而 $m = tab$, 故 $ab \mid m$.

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 $a_1, \cdots, a_n$ 的**最小公倍数**, 记作 $[a_1, \cdots, a_n]$.

定理 1.2.11

设 a, b 是两个互素的正整数, 则

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

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

证: (i) 设 $b \mid m$, 则存在整数 k 使得 $m = k \cdot b$. 又 $a \mid m$, 即 $a \mid k \cdot b$, 而 $(a, b) = 1$, 由定理 1.2.9 知, $a \mid k$, 则存在整数 t 使得 $k = t \cdot a$. 从而 $m = tab$, 故 $ab \mid m$.

(ii) 显然 ab 是 a, b 的公倍数. 又由 (i) 知, ab 是 a, b 的公倍数中的最小正整数, 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 1.2.17 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 $[p, q] = pq$.

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

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

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

证：令 $d = (a, b)$, 根据定理 1.2.7, 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, $[a, b] = \frac{a \cdot b}{d}$, 即 (ii) 成立.

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

证：令 $d = (a, b)$, 根据定理 1.2.7, 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, $[a, b] = \frac{a \cdot b}{d}$, 即 (ii) 成立.

再由 $\frac{a}{d} \mid \frac{m}{d}$, $\frac{b}{d} \mid \frac{m}{d}$ 且 $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$ 得到,

$$\frac{a}{d} \cdot \frac{b}{d} \Big| \frac{m}{d},$$

从而 $\frac{a \cdot b}{d} \mid m$, 即 (i) 成立.

定理 1.2.13

设 $a_1, \cdots, a_n$ 是 n 个整数. 令

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

则 $[a_1, \cdots, a_n] = m_n$.

定理 1.2.13

设 $a_1, \cdots, a_n$ 是 n 个整数. 令

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

则 $[a_1, \cdots, a_n] = m_n$.

例 1.2.19　计算最小公倍数 $[12, 25, 100, 256]$.

定理 1.2.13

设 $a_1, \cdots, a_n$ 是 n 个整数. 令

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

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

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

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

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

定理 1.2.13

设 $a_1, \cdots, a_n$ 是 n 个整数. 令

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

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 $a_1, \cdots, a_n$ 是正整数. 如果 $a_1 \mid m, a_2 \mid m, \cdots, a_n \mid m$, 则

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

定理 1.2.14

设 $a_1, \cdots, a_n$ 是正整数. 如果 $a_1 \mid m, a_2 \mid m, \cdots, a_n \mid m$, 则

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

证：对 n 作数学归纳法.

$n = 2$ 时, 命题就是定理 1.2.12 (i), 结论成立.

假设 $n-1 (n \geqslant 3)$ 时, 结论成立. 即

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

对于 n, 根据定理 1.2.13, 有 $[m_{n-1}, a_n] = [a_1, a_2, \cdots, a_n]$. 而根据题设 $a_n \mid m$, 故有

$$[m_{n-1}, a_n] \mid m.$$

故结论成立.

目录

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.

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.

目录

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

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

其中 p_i 是素数, 并且若 $n = q_1 \cdots q_t,\ q_1 \leqslant \cdots \leqslant q_t$, 其中 q_j 是素数, 则 $s = t,\ p_i = q_i, 1 \leqslant i \leqslant s.$

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

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

其中 p_i 是素数, 并且若 $n = q_1 \cdots q_t,\ q_1 \leqslant \cdots \leqslant q_t$, 其中 q_j 是素数, 则 $s = t,\ p_i = q_i, 1 \leqslant i \leqslant s$.

证: 首先用数学归纳法证明表达式 (1.3.1) 成立.

$n = 2$ 时, 式 (1.3.1) 显然成立.

假设对于 $< n$ 的正整数, 式 (1.3.1) 成立.

对于正整数 n, 若 n 是素数, 则式 (1.3.1) 对 n 成立. 若 n 是合数, 则存在正整数 n_1, n_2 使得 $n = n_1 \cdot n_2,\ 1 < n_1 < n, 1 < n_2 < n$. 根据归纳假设, 有 $n_1 = p'_1 \cdots p'_u,\ n_2 = p'_{u+1} \cdots p'_s$. 于是, $n = p'_1 \cdots p'_u \cdot p'_{u+1} \cdots p'_s$. 适当改变 p'_i 的次序即得式 (1.3.1), 故式 (1.3.1) 对 n 成立.

再证明表达式是唯一的.

若还有 $n = q_1 \cdots q_t,\ q_1 \leqslant \cdots \leqslant q_t$, 其中 q_j 是素数, 则

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

因此, $p_1 \mid q_1 \cdots q_t$. 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, $p_1 \leqslant p_k = q_1 \leqslant q_j = p_1$. 进而, $p_1 = q_1$.

再证明表达式是唯一的.

若还有 $n = q_1 \cdots q_t,\ q_1 \leqslant \cdots \leqslant q_t$, 其中 q_j 是素数, 则

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

因此, $p_1 \mid q_1 \cdots q_t$. 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, $p_1 \leqslant p_k = q_1 \leqslant q_j = p_1$. 进而, $p_1 = q_1$.

将式 (1.3.2) 的两端同时消除 p_1, 得

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

同理可推出 $p_2 = q_2$. 以此类推, 可得到 $p_3 = q_3, \cdots, q_s = p_t$ 以及 $s = t$.

再证明表达式是唯一的.

若还有 $n = q_1 \cdots q_t$, $q_1 \leqslant \cdots \leqslant q_t$, 其中 q_j 是素数, 则

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

因此, $p_1 \mid q_1 \cdots q_t$. 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, $p_1 \leqslant p_k = q_1 \leqslant q_j = p_1$. 进而, $p_1 = q_1$.

将式 (1.3.2) 的两端同时消除 p_1, 得

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

同理可推出 $p_2 = q_2$. 以此类推, 可得到 $p_3 = q_3, \cdots, q_s = p_t$ 以及 $s = t$.

例 1.3.1　写出整数 12, 25, 100, 256 的因数分解式.

再证明表达式是唯一的.

若还有 $n = q_1 \cdots q_t$, $q_1 \leqslant \cdots \leqslant q_t$, 其中 q_j 是素数, 则

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

因此, $p_1 \mid q_1 \cdots q_t$. 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, $p_1 \leqslant p_k = q_1 \leqslant q_j = p_1$. 进而, $p_1 = q_1$.

将式 (1.3.2) 的两端同时消除 p_1, 得

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

同理可推出 $p_2 = q_2$. 以此类推, 可得到 $p_3 = q_3, \cdots, q_s = p_t$ 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, 有

$$12 = 2 \cdot 2 \cdot 3, \qquad 25 = 5 \cdot 5,$$

$$100 = 2 \cdot 2 \cdot 5 \cdot 5, \quad 256 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 2.$$

将相同的素数的乘积写成素数幂的形式, 那么定理 1.3.2 可表述成:

定理 1.3.3

任一整数 $n > 1$ 可以唯一地表示成

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

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

将相同的素数的乘积写成素数幂的形式, 那么定理 1.3.2 可表述成:

定理 1.3.3

任一整数 $n > 1$ 可以唯一地表示成

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

其中 $p_i < p_j$ $(i < j)$ 是素数. 这里, 式 (1.3.3) 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.

将相同的素数的乘积写成素数幂的形式, 那么定理 1.3.2 可表述成:

定理 1.3.3

任一整数 $n > 1$ 可以唯一地表示成

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

其中 $p_i < p_j$ $(i < j)$ 是素数. 这里, 式 (1.3.3) 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, 有

$$12 = 2^2 \cdot 3, \qquad 49 = 5^2,$$
$$100 = 2^2 \cdot 5^2, \quad 256 = 2^8.$$

接下来, 利用算术基本定理进一步探讨整数的性质.

定理 1.3.4

设 n 是大于 1 的一个整数, 且有标准分解式

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

则 d 是 n 的正因数当且仅当 d 有因数分解式

$$d = p_1^{\beta_1} \cdots p_s^{\beta_s},\ \alpha_i \geqslant \beta_i \geqslant 0, i = 1, \cdots, s. \tag{1.3.4}$$

接下来, 利用算术基本定理进一步探讨整数的性质.

定理 1.3.4

设 n 是大于 1 的一个整数, 且有标准分解式

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

则 d 是 n 的正因数当且仅当 d 有因数分解式

$$d = p_1^{\beta_1} \cdots p_s^{\beta_s},\ \alpha_i \geqslant \beta_i \geqslant 0, i = 1, \cdots, s. \tag{1.3.4}$$

证：必要性. 设 $d \mid n$, 且 d 有因数分解式

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

则一定有 $\alpha_i \geqslant \beta_i, i = 1, \cdots, s.$

(事实上, 若不然, 则存在 $1 \leqslant i \leqslant s$ 使得 $\alpha_i < \beta_i$. 不妨设, $\alpha_1 < \beta_1$. 根据 $d \mid n$ 及 $p_1^{\beta_1} \mid d$, 可得 $p_1^{\beta_1} \mid p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$. 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 $j, 2 \leqslant j \leqslant k$ 使得 $p_1 \mid p_j$. 这不可能. 故式 (1.3.4) 成立.)

接下来, 利用算术基本定理进一步探讨整数的性质.

定理 1.3.4

设 n 是大于 1 的一个整数, 且有标准分解式

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

则 d 是 n 的正因数当且仅当 d 有因数分解式

$$d = p_1^{\beta_1} \cdots p_s^{\beta_s},\ \alpha_i \geqslant \beta_i \geqslant 0, i = 1, \cdots, s. \tag{1.3.4}$$

证：必要性. 设 $d \mid n$, 且 d 有因数分解式

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

则一定有 $\alpha_i \geqslant \beta_i, i = 1, \cdots, s.$

(事实上, 若不然, 则存在 $1 \leqslant i \leqslant s$ 使得 $\alpha_i < \beta_i$. 不妨设, $\alpha_1 < \beta_1$. 根据 $d \mid n$ 及 $p_1^{\beta_1} \mid d$, 可得 $p_1^{\beta_1} \mid p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$. 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 $j, 2 \leqslant j \leqslant k$ 使得 $p_1 \mid p_j$. 这不可能. 故式 (1.3.4) 成立.)

充分性. 令 $n' = p_1^{\alpha_1 - \beta_1} \cdots p_s^{\alpha_s - \beta_s}$, 则有 $n = n' \cdot d$. 故 $d \mid n$.

例 1.3.3 设正整数 n 有因数分解式

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

则 n 的因数个数为

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

例 1.3.3 设正整数 n 有因数分解式

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

则 n 的因数个数为

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

证：设 $d \mid n$ 且 d 有因数分解式

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

因为 β_1 的变化范围是 $0 \sim \alpha_1$, 共 $1 + \alpha_1$ 个值,

$\cdots$,

β_s 的变化范围是 $0 \sim \alpha_s$, 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, 且都有因数分解式

$$a = p_1^{\alpha_1} \cdots p_s^{\alpha_s},\ \alpha_i \geqslant 0, i = 1, \cdots, s,$$

$$b = p_1^{\beta_1} \cdots p_s^{\beta_s},\ \beta_i \geqslant 0, i = 1, \cdots, s.$$

则 a 和 b 的最大公因数和最小公倍数分别有因数分解式

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

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

定理 1.3.5

设 a, b 是两个正整数, 且都有因数分解式

$$a = p_1^{\alpha_1} \cdots p_s^{\alpha_s},\ \alpha_i \geqslant 0, i = 1, \cdots, s,$$

$$b = p_1^{\beta_1} \cdots p_s^{\beta_s},\ \beta_i \geqslant 0, i = 1, \cdots, s.$$

则 a 和 b 的最大公因数和最小公倍数分别有因数分解式

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

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

证：根据定理 1.3.4 知, 整数 $d = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$ 满足最大公因数的数学定义, 所以 $(a, b) = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$. 同样, 整数 $m = p_1^{\delta_1} \cdots p_s^{\delta_s}$ 满足最小公倍数的数学定义, 所以 $[a, b] = p_1^{\delta_1} \cdots p_s^{\delta_s}$.

定理 1.3.5

设 a,b 是两个正整数, 且都有因数分解式

$$a = p_1^{\alpha_1} \cdots p_s^{\alpha_s},\ \alpha_i \geqslant 0, i = 1, \cdots, s,$$

$$b = p_1^{\beta_1} \cdots p_s^{\beta_s},\ \beta_i \geqslant 0, i = 1, \cdots, s.$$

则 a 和 b 的最大公因数和最小公倍数分别有因数分解式

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

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

证：根据定理 1.3.4 知, 整数 $d = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$ 满足最大公因数的数学定义, 所以 $(a,b) = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$. 同样, 整数 $m = p_1^{\delta_1} \cdots p_s^{\delta_s}$ 满足最小公倍数的数学定义, 所以 $[a,b] = p_1^{\delta_1} \cdots p_s^{\delta_s}$.

推论 1.3.1

设 a,b 是两个正整数, 则 $(a,b)[a,b] = ab$.

定理 1.3.5

设 a,b 是两个正整数, 且都有因数分解式

$$a = p_1^{\alpha_1} \cdots p_s^{\alpha_s},\ \alpha_i \geqslant 0, i = 1, \cdots, s,$$

$$b = p_1^{\beta_1} \cdots p_s^{\beta_s},\ \beta_i \geqslant 0, i = 1, \cdots, s.$$

则 a 和 b 的最大公因数和最小公倍数分别有因数分解式

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

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

证：根据定理 1.3.4 知, 整数 $d = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$ 满足最大公因数的数学定义, 所以 $(a,b) = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$. 同样, 整数 $m = p_1^{\delta_1} \cdots p_s^{\delta_s}$ 满足最小公倍数的数学定义, 所以 $[a,b] = p_1^{\delta_1} \cdots p_s^{\delta_s}$.

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 α, β, 有 $\min(\alpha,\beta) + \max(\alpha,\beta) = \alpha + \beta$.

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

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, 有

$$12 = 2^2 \cdot 3, \qquad 49 = 5^2,$$

$$100 = 2^2 \cdot 5^2, \quad 256 = 2^8.$$

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, 有

$$12 = 2^2 \cdot 3, \qquad 49 = 5^2,$$
$$100 = 2^2 \cdot 5^2, \quad 256 = 2^8.$$

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.

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, 有

$$12 = 2^2 \cdot 3, \qquad 49 = 5^2,$$

$$100 = 2^2 \cdot 5^2, \quad 256 = 2^8.$$

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, 给出如下结果. 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

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

利用整数的唯一因数分解式, 给出如下结果. 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

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

证：将整数 a,b 进行因数分解, 得

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

其中 $\alpha_i \geqslant \beta_i \geqslant 0, i = 1, \cdots, t;\ \beta_i > \alpha_i \geqslant 0, i = t+1, \cdots, s.$

——不再按素因数大小进行排序，而按 a,b 的素因数指数大小进行分类.

取

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

则整数 a', b' 即为所求.

利用整数的唯一因数分解式, 给出如下结果. 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

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

证：将整数 a,b 进行因数分解, 得

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

其中 $\alpha_i \geqslant \beta_i \geqslant 0, i = 1, \cdots, t;\ \beta_i > \alpha_i \geqslant 0, i = t+1, \cdots, s.$

——不再按素因数大小进行排序，而按 a,b 的素因数指数大小进行分类.

取

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

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

本课作业

1. 利用广义欧几里德除法计算整数 $a = 2394, b = 5567$ 的最大公因数 (a, b), 并求出整数 s, t, 使得 $(a, b) = sa + tb$. 进一步, 计算 a, b 的最小公倍数 $[a, b]$.

2. 证明 $((a, b), b) = (a, b)$.

3. 若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.

4. 利用算术基本定理计算整数 $420, 192, 450, 969$ 的最大公因子与最小公倍数.

5. 设 a, b 为正整数, 证明: 若 $[a, b] = (a, b)$, 则 $a = b$.

交流与讨论

电子邮箱：

陈秀波：xb_chen@bupt.edu.cn

徐国胜：guoshengxu@bupt.edu.cn

金正平：zhpjin@bupt.edu.cn