第二十章  初等数论

本章简要地介绍了初等数论的基础知识，共分六节。前五节讨论了整数的性质与辗转相除法，连分数与费波那奇序列、同余式与孙子定理，介绍了几种重要的数论函数和麦比乌斯变换，并列出几类不可约多项式的判别方法。最后一节对代数数等基本概念和性质作了简单的介绍。

§1  整数

[整数部分与分数部分]  设\( \alpha \)为一实数，不超过\( \alpha \)的最大整数称为\( \alpha \)的整数部分，记作\( \lfloor \alpha \rfloor \)。

而\( \{ \alpha \} \)称为\( \alpha \)的分数部分。

例如  \( \lfloor 1 \rfloor = 1 \),  \( \lfloor 2.3 \rfloor = 2 \),  \( \lfloor -3.5 \rfloor = -4 \) 等等

整数部分具有下列关系式:

\[
\lfloor \alpha \rfloor \leq \alpha < \lfloor \alpha \rfloor + 1
\]

\[
\left\lfloor \frac{n\alpha}{n} \right\rfloor = \lfloor \alpha \rfloor, n \text{为自然数}
\]

\[
\lfloor \alpha \rfloor + \left\lfloor \frac{\alpha + 1}{n} \right\rfloor + \cdots + \left\lfloor \frac{\alpha + n-1}{n} \right\rfloor = \lfloor n\alpha \rfloor, n \text{为自然数}
\]

\[
\lfloor 2\alpha \rfloor + [2\beta] \geq \lfloor \alpha \rfloor + [\alpha + \beta] + [\beta]
\]

\[
\lfloor \alpha \rfloor - [\beta] = [\alpha - \beta] \text{或} [\alpha - \beta] + 1
\]

注意，在计算机程序中的“取整运算”与这里的“整数部分”意义是有差别的：当\( \alpha \geq 0 \)时是一致的；当\( \alpha < 0 \)时就不一致。例如\( \lfloor -3.5 \rfloor = -4 \)，但计算机上\(-3.5\)取整后为\(-3\)。

[整除性]  若有一整数\( c \)使得整数\( a \)与\( b \)之间适合于

\[
a = bc
\]

则称\( b \)可整除\( a \)，记作\( b \mid a \)。这时\( a \)称为\( b \)的倍数，\( b \)称为\( a \)的因数(或约数)。

若\( b \)不能整除\( a \)，则记作\( b \nmid a \)。

整除性具有下列性质(下列各式**b ≠ 0, c ≠ 0**):

1°  若\( b \mid a \), \( c \mid b \)，则\( c \mid a \)；

2°  若\( b \mid a \)，则\( bc \mid ac \)；

3°  若\( c \mid d, c \mid e \)，则对于任意整数\( m, n \)有

\[
c \mid d m + ea
\]

4°  若\( b \)是\( a \)的真因数(即\( b \neq 1, a \)), 则

\[
1 < |b| < |a|
\]

[素数与爱拉托斯散筛法]  恰有 1 和本身两个自然数为其因数的大于 1 的整数称为素数，记作\( p \)。除 2 为偶数外，其余素数都是奇数。

素数具有性质:
1° 素数有无限多个. 如果不超过自然数 $n$ 的素数个数记作 $\pi(n)$, 则当 $n \geq 2$ 时, 有
$$\frac{1}{8} \frac{n}{\log n} \leq \pi(n) \leq 12 \frac{n}{\log n}.$$ 进一步有
$$\lim_{n \to \infty} \frac{\pi(n)}{n} = 1$$

2° 设 $p$ 为素数, 若 $p | ab$, 则 $p | a$ 或 $p | b$.

3° $n!$ 中含素数 $p$ 的方次数等于
$$\left[ \frac{n}{p} \right] + \left[ \frac{n}{p^2} \right] + \left[ \frac{n}{p^3} \right] + \cdots$$

4° 若 $n \leq N$ 为正整数, 它不能被不超过 $\sqrt{N}$ 的所有素数所整除, 则 $n$ 必为素数. 这种判别自然数是否为素数的方法称为爱拉托斯散筛法. 由此法可建立素数表.

[唯一分解定理] 大于 $1$ 的自然数都可唯一地分解为素数幂的积. 设 $n > 1$, 为自然数, 则 $n$ 可唯一地表为
$$n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s},$$
$$a_1 > 0, a_2 > 0, \cdots, a_s > 0 \quad (\text{为自然数})$$
$$p_1 < p_2 < \cdots < p_s \quad (\text{为素数})$$

这称为 $n$ 的标准分解式. $n$ 所含不同素因数的个数 $s$ 不超过 $\frac{\log n}{\log 2}$.

显然, 任意自然数 $n$ 可表为
$$n = 2^k (2m+1) \quad (k, m \text{ 为自然数或零})$$

这种表达式是唯一的.

[麦森数] 整数
$$M_p = 2^p - 1 \quad (p \text{ 为素数})$$

为素数者称为麦森数, 至今仅发现 27 个, 即
$$p = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 167, 179, 2203, 2281, 23209, 24037, 29443, 31261, 38593, 69725, 134669, 209967, 320321, 636961, 904637, 1257787$$

是否有无穷个麦森数还未证明.

[费马数] 整数
$$F_n = 2^{2^n} + 1 \quad (n \text{ 为自然数})$$

称为费马数. 至今只发现 5 个费马数为素数, 即
$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$$

下列 46 个费马数皆非素数:
$$n = 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 18, 19, 21, 23, 25, 26, 27, 30, 32, 36, 38, 39, 42, 52, 55, 58, 63, 73, 77, 81, 117, 125, 144, 150, 207, 226, 228, 250, 267, 268, 284, 316, 452, 1945$$

数论中通常把自然对数 $\ln x$ 记作 $\log x$. 
辗转相除法

每一个整数 $a$ 可以唯一地通过正整数 $b$ 表为

$$a = bq + r, 0 \leq r < b$$

式中 $q$ 称为 $a$ 被 $b$ 除所得的不完全商，$r$ 称为 $a$ 被 $b$ 除所得的余数。辗转相除法是指下列一串有限个等式:

$$\begin{align*}
\left\{ \begin{array}{l}
\ a = b_0 q_0 + r_0, & 0 < r_0 < b_0 \\
\ b = q_0 a_1 + r_1, & 0 < r_1 < q_0 \\
\ q_0 = q_1 a_2 + r_2, & 0 < r_2 < q_0 \\
\ r_2 = q_2 a_3 + r_3, & 0 < r_3 < q_2 \\
\ &= \cdots \\
\ r_{N-2} = q_{N-2} a_{N-1} + r_{N-1}, & 0 < r_{N-1} < q_{N-2} \\
\ r_{N-1} = q_{N-1} a_N \\
\end{array} \right. \quad (1)
\end{align*}$$

例 1 设 $a = 525, b = 231$，根据 (1) 式可列出下面的算式和草式:

<table>
<thead>
<tr>
<th>算式</th>
<th>草式</th>
</tr>
</thead>
<tbody>
<tr>
<td>525 = 231·2 + 63</td>
<td>a1</td>
</tr>
<tr>
<td>231 = 63·3 + 42</td>
<td>525 ↓</td>
</tr>
<tr>
<td>63 = 42·1 + 21</td>
<td>231 2 462</td>
</tr>
<tr>
<td>42 = 21·2</td>
<td>189 3 63</td>
</tr>
<tr>
<td></td>
<td>42 1 42</td>
</tr>
<tr>
<td></td>
<td>42 2 21</td>
</tr>
<tr>
<td></td>
<td>0</td>
</tr>
</tbody>
</table>

最大公因数与最小公倍数

设 $a, b$ 为整数，既能整除 $a$，又能整除 $b$ 的正整数称为 $a, b$ 的公因数，其最大者称为 $a, b$ 的最大公因数，记作 $(a, b)$，即

$$(a, b) = \max\{c \mid c|a, c|b\}$$

特别当 $(a, b) = 1$ 时，称 $a, b$ 互素。

设 $a, b$ 为正整数，$a, b$ 都能整除的正整数称为 $a, b$ 的公倍数，其最小者称为 $a, b$ 的最小公倍数，记作 $[a, b]$，即

$$[a, b] = \min\{d \mid d|a, b|a\}$$

设 $a_1, a_2, \cdots, a_n$ 为 $n$ 个正整数，用归纳法定义其最大公因数为

$$(a_1, a_2, \cdots, a_n) = ((a_1, \cdots, a_{n-1}), a_n)$$

其最小公倍数为

$$[a_1, a_2, \cdots, a_n] = [(a_1, \cdots, a_{n-1}), a_n]$$

最大公因数与最小公倍数具有下列性质:

1. 存在整数 $x, y$ 使得 $(a, b) = ax + by$。并可由辗转相除法具体求出 $x, y$，使 $(a, b)$ 也由辗转相除法的一串等式 (1) 得到，即

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{N-1}, r_N) = r_N$$

* 我国古代数学家秦九韶于 1247 年在《数书九章》中讨论过辗转相除法（也称欧几里得算法）。

* 国外书刊中，$a, b$ 的最大公因数常记为 $\text{g.c.d.}(a, b)$，$a, b$ 的最小公倍数常记为 $\text{l.c.m.}(a, b)$。
例2 由例1得\((525,231)=21\). 因为由例1的算式有
\[
\begin{align*}
21 &= 63 - 2 \cdot 1 = 63 - (231 - 63 \cdot 3) \cdot 1 \\
&= 63 \cdot 4 - 231 = (525 - 231) \cdot 4 - 231 \\
&= 525 \cdot 4 - 231 \cdot 9
\end{align*}
\]
所以得到 \(x=4, y=-9\).

2° 对任意二整数 \(x,y\), 必有 \((a,b)\mid ax + by\).

3° 若 \(d\mid a\), \(d\mid b\), 则 \(d\mid (a,b)\).

4° 若 \(c > 0\), \((a,b) = d\), 则 \((ac,bc) = dc\).

若 \(c > 0\), \(c\mid d\), 则 \(\frac{a}{c}, \frac{b}{c} = \frac{d}{c}\).

5° 若 \(a,b\) 为二正整数, \(p_1, \ldots, p_s\) 为它们的素因数, 且标准分解式分别为
\[
\begin{align*}
a &= p_1^{a_1} \cdots p_s^{a_s}, & a_i \geq 0 & (1 \leq i \leq s) \\
b &= p_1^{b_1} \cdots p_s^{b_s}, & b_i \geq 0 & (1 \leq i \leq s) \\
p_1 < \cdots < p_s
\end{align*}
\]
则
\[
\begin{align*}
(a,b) &= p_1^{c_1} \cdots p_s^{c_s}, & c_i = \min\{a_i, b_i\} & (1 \leq i \leq s) \\
[a,b] &= p_1^{e_1} \cdots p_s^{e_s}, & e_i = \max\{a_i, b_i\} & (1 \leq i \leq s)
\end{align*}
\]

6° \([a,b] = ab\)

7° 若 \(a_1, a_2, \ldots, a_n\) 为互素的正整数, 即 \((a_1, a_2, \ldots, a_n) = 1\), 则
\[(a_1, a_2) \cdots (a_1, a_n) \leq a_1^{n-2}\]