第 1 章　整数的可除性

信息通信技术的广泛应用需要信息的数字化. 在保证信息的安全性和有效性 (如公钥密码系统即 RSA) 时往往要用到整数的算术性质, 所以本章将讨论整数的算术性质、基本理论和方法, 特别是整除、因数、素数、最大公因数、最小公倍数以及欧几里得除法和广义欧几里得除法, 最后给出算术基本定理和素数定理.

1.1　整除的概念、欧几里得除法

1.1.1　整除的概念

本节考虑关于整数的一些基本概念和性质: 整除和欧几里得除法.

首先考虑具有一般意义的整除定义, 它只涉及乘法运算.

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

$$a = q \cdot b \tag{1.1}$$

成立, 就称 b **整除** a 或者 a 被 b 整除, 记作 $b \mid a$, 并把 b 叫做 a 的 **因数**, 把 a 叫做 b 的 **倍数**. 人们常将 q 写成 a/b 或 $\dfrac{a}{b}$. 否则, 就称 b 不能整除 a, 或者 a 不能被 b 整除, 记作 $b \nmid a$.

因为整数乘法运算的可交换性, 又有 $a = b \cdot q$, 所以 q 也是 a 的因数. 此外, 在不会混淆的情况下, 乘法 $a \cdot b$ 常简记为 ab.

注

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

(2) 当 b 遍历整数 a 的所有因数时, $\dfrac{a}{b}$ 也遍历整数 a 的所有因数.

例 1.1.1　$30 = 15 \cdot 2 = 10 \cdot 3 = 6 \cdot 5$.

将 2, 3, 5 分别整除 30 或 30 被 2, 3, 5 分别整除, 记作 $2 \mid 30,\ 3 \mid 30,\ 5 \mid 30$. 这时, 2, 3, 5 都是 30 的因数, 30 是 2, 3, 5 的倍数. 同时, 也有 $15 \mid 30,\ 10 \mid 30,\ 6 \mid 30$.

30 的所有因数是 $\{\pm 1,\ \pm 2,\ \pm 3,\ \pm 5,\ \pm 6,\ \pm 10,\ \pm 15,\ \pm 30\}$,

或是 $\{\mp 1,\ \mp 2,\ \mp 3,\ \mp 5,\ \mp 6,\ \mp 10,\ \mp 15,\ \mp 30\}$,

或是 $\Big\{ \pm 30 = \dfrac{30}{\pm 1},\ \pm 15 = \dfrac{30}{\pm 2},\ \pm 10 = \dfrac{30}{\pm 3},\ \pm 6 = \dfrac{30}{\pm 5},\ \pm 5 = \dfrac{30}{\pm 6},\ \pm 3 = \dfrac{30}{\pm 10},$
$\pm 2 = \dfrac{30}{\pm 15},\ \pm 1 = \dfrac{30}{\pm 30} \Big\}$.

列表就是:

d	± 1	± 2	± 3	± 5	± 6	± 10	± 15	± 30
$-d$	∓ 1	∓ 2	∓ 3	∓ 5	∓ 6	∓ 10	∓ 15	∓ 30
$\dfrac{n}{d}$	± 30	± 15	± 10	± 6	± 5	± 3	± 2	± 1

又例如: $7 \mid 84,\ -7 \mid 84,\ 5 \mid 20,\ 19 \mid 171,\ 3 \nmid 8,\ 5 \nmid 12,\ 13 \mid 0,\ 11 \mid 11$.

根据定义有:

- 0 是任何非零整数的倍数.
- 1 是任何整数的因数.
- 任何非零整数 a 是其自身的倍数, 也是其自身的因数.

例 1.1.2 设 $a,\ b$ 为整数. 若 $b \mid a$, 则 $b \mid (-a),\ (-b) \mid a,\ (-b) \mid (-a)$.

证 设 $b \mid a$, 则存在整数 q 使得 $a = q \cdot b$. 因而,

$$(-a) = (-q) \cdot b, \quad a = (-q) \cdot (-b), \quad (-a) = q \cdot (-b).$$

因为 $-q,\ q$ 都是整数, 所以根据整除的定义有

$$b \mid (-a), \ \ (-b) \mid a, \ \ (-b) \mid (-a).$$

证毕.

整除具有传递性, 即

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

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

$$a = q_1 \cdot b, \quad b = q_2 \cdot c.$$

因此, 有

$$a = q_1 \cdot b = q_1 \cdot (q_2 \cdot c) = q \cdot c.$$

因为 $q = q_1 \cdot q_2$ 是整数, 所以根据整除的定义, 有 $c \mid a$. 证毕.

例 1.1.3 因为 $7 \mid 42,\ 42 \mid 84$, 所以 $7 \mid 84$.

在加法、减法运算中, 整除的性质是保持的.

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

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

$$a = q_1 \cdot c, \quad b = q_2 \cdot c.$$

因此,

$$a \pm b = q_1 \cdot c \pm q_2 \cdot c = (q_1 \pm q_2) \cdot c.$$

因为 $q_1 \pm q_2$ 是整数, 所以 $a \pm b$ 被 c 整除. 证毕.

例 1.1.4 因为 $7 \mid 14,\ 7 \mid 84$, 所以

$$7 \mid (84 + 14) = 98, \quad 7 \mid (84 - 14) = 70.$$

进一步, 在整数 a, b 的线性组合中, 整除的性质是保持的.

定理 1.1.3 设 $a,\ b,\ c \neq 0$ 是三个整数. 若 $c \mid a,\ c \mid b$, 则对任意整数 s、t, 有 $c \mid (s \cdot a + t \cdot b)$.

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

$$a = q_1 \cdot c, \quad b = q_2 \cdot c.$$

因此,

$$s \cdot a + t \cdot b = s \cdot (q_1 \cdot c) + t \cdot (q_2 \cdot c) = (s \cdot q_1 + t \cdot q_2) \cdot c.$$

因为 $s \cdot q_1 + t \cdot q_2$ 是整数, 所以 $s \cdot a + t \cdot b$ 被 c 整除. 证毕.

例 1.1.5 因为 $7 \mid 14,\ 7 \mid 21$, 所以

$$7 \mid (3 \cdot 21 - 4 \cdot 14) = 7, \quad 7 \mid (3 \cdot 21 + 4 \cdot 14) = 119.$$

例 1.1.6 设 $a,\ b,\ c \neq 0$ 是三个整数, $c \mid a,\ c \mid b$. 如果存在整数 $s,\ t$, 使得 $s \cdot a + t \cdot b = 1$, 则 $c = \pm 1$.

证 设 $c \mid a,\ c \mid b$, 因为存在整数 $s,\ t$, 使得 $s \cdot a + t \cdot b = 1$, 根据定理 1.1.3, 有

$$c \mid s \cdot a + t \cdot b = 1.$$

因此, $c = \pm 1$. 证毕.

定理 1.1.3 可推广为多个整数的线性组合.

定理 1.1.4 设整数 $c \neq 0$. 若整数 $a_1,\ \cdots,\ a_n$ 都是整数 c 的倍数, 则对任意 n 个整数 $s_1,\ \cdots,\ s_n$, 整数

$$s_1 a_1 + \cdots + s_n a_n$$

是 c 的倍数.

证 设 $c \mid a_i,\ \ 1 \leqslant i \leqslant n$, 那么存在 n 个整数 $q_i,\ \ 1 \leqslant i \leqslant n$ 使得

$$a_i = q_i \cdot c, \quad 1 \leqslant i \leqslant n.$$

因此,

$$s_1 a_1 + \cdots + s_n a_n = s_1 (q_1 \cdot c) + \cdots + s_n (q_n \cdot c) = (s_1 q_1 + \cdots + s_n q_n) \cdot c$$

因为 $s_1 q_1 + \cdots + s_n q_n$ 是整数, 所以 $s_1 a_1 + \cdots + s_n a_n$ 能被 c 整除. 证毕.

例 1.1.7 因为 $7 \mid 14,\ 7 \mid 21,\ 7 \mid 35$, 所以

$$7 \mid (5 \cdot 21 + 4 \cdot 14 - 3 \cdot 35) = 56.$$

定理 1.1.5 设 $a,\ b$ 都是非零整数. 若 $a \mid b,\ b \mid a$, 则 $a = \pm b$.

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

$$a = q_1 \cdot b, \quad b = q_2 \cdot a.$$

从而,

$$a = q_1 \cdot b = q_1 \cdot (q_2 \cdot a) = (q_1 \cdot q_2)\, a \qquad 或 \qquad (q_1 \cdot q_2 - 1)\, a = 0.$$

因为 $a \neq 0$, 根据整数乘法的性质, 有 $q_1 \cdot q_2 = 1$. 但 $q_1,\ q_2$ 都是整数, 所以 $q_1 = q_2 = \pm 1$. 进而, $a = \pm b$. 证毕.

前面考虑了整除和因数, 现在考虑对于乘法的最小整数, 也就是不能继续分解的整数 (± 1 除外), 即下面的素数.

定义 1.1.2 设整数 $n \neq 0,\ \pm 1$. 如果除了显然因数 ± 1 和 $\pm n$ 外, n 没有其他因数, 那么, n 就叫做 **素数** (或**质数**或**不可约数**), 否则, n 叫做 **合数**.

当整数 $n \neq 0,\ \pm 1$ 时, n 和 $-n$ 同为素数或合数. 因此, 若没有特别声明, 素数总是指正整数, 通常写成 p.

例 1.1.8 整数 $2,\ 3,\ 5,\ 7$ 都是素数; 而整数 $4,\ 6,\ 10,\ 15,\ 21$ 都是合数.

下面要证明每个合数必有素因子.

定理 1.1.6 设 n 是一个正合数, p 是 n 的一个大于 1 的最小正因数, 则 p 一定是素数, 且 $p \leqslant \sqrt{n}$.

证 反证法. 如果 p 不是素数, 则存在整数 q, $1 < q < p$, 使得 $q \mid p$. 但 $p \mid n$, 根据整除的传递性 (定理 1.1.1), 有 $q \mid n$. 这与 p 是 n 的最小正因数矛盾. 所以, p 是素数.

因为 n 是合数, 所以存在整数 n_1 使得

$$n = n_1 \cdot p, \quad 1 < p \leqslant n_1 < n.$$

因此, $p^2 \leqslant n$. 故 $p \leqslant \sqrt{n}$. 证毕.

注 定理 1.1.6 表明, 素数为乘法的最小单元, 并且整数可以表示成素数的乘积 (定理 1.6.1).

1.1.2 Eratoshenes 筛法

根据定理 1.1.6, 合数 n 的最小因数 p 为素数, 且 $p \leqslant \sqrt{n}$. 由此, 可立即得到一个判断整数是否为素数的法则 (只用到整数的乘法运算).

定理 1.1.7 设 n 是正整数. 如果对所有的素数 $p \leqslant \sqrt{n}$, 都有 $p \nmid n$, 则 n 一定是素数.

应用定理 1.1.7, 可得到一个寻找素数的确定性方法, 通常叫做 **平凡除法** 或 **厄拉托塞师 (Eratosthenes) 筛法**.

下面给出具体的描述.

对任意给定的正整数 N , 要求出所有不超过 N 的素数. 列出 N 个整数, 从中删除不大于 $\sqrt{N}$ 的所有素数 p_1, p_2, $\cdots$, p_k 的倍数 (除素数 p_1, p_2 $\cdots$, p_k 外). 具体地是依次删除,

$$\begin{aligned}
p_1 \text{ 的倍数}: &\quad 2 \cdot p_1, \quad 3 \cdot p_1, \quad \cdots, \quad \left[\frac{N}{p_1}\right] \cdot p_1; \\
p_2 \text{ 的倍数}: &\quad 2 \cdot p_2, \quad 3 \cdot p_2, \quad \cdots, \quad \left[\frac{N}{p_2}\right] \cdot p_2; \\
&\vdots \\
p_k \text{ 的倍数}: &\quad 2 \cdot p_k, \quad 3 \cdot p_k, \quad \cdots, \quad \left[\frac{N}{p_k}\right] \cdot p_k.
\end{aligned}$$

余下的整数 (不包括 1) 就是所要求的不超过 N 的素数 (符号 [ ] 的解释见定义 1.1.4).

例 1.1.9 求出所有不超过 $N = 100$ 的素数.

解 因为 $N = 100$, 所以不大于 $\sqrt{N} = 10$ 的所有素数为 2, 3, 5, 7, 所以依次删除 2, 3, 5, 7 的倍数,

$$\begin{array}{lllllll}
2 \cdot 2, & 3 \cdot 2, & 4 \cdot 2, & \cdots, & 49 \cdot 2, & 50 \cdot 2 \\
2 \cdot 3, & 3 \cdot 3, & 4 \cdot 3, & \cdots, & 32 \cdot 3, & 33 \cdot 3 \\
2 \cdot 5, & 3 \cdot 5, & 4 \cdot 5, & \cdots, & 19 \cdot 5, & 20 \cdot 5 \\
2 \cdot 7, & 3 \cdot 7, & 4 \cdot 7, & \cdots, & 13 \cdot 7, & 14 \cdot 7.
\end{array}$$

余下的整数 (不包括 1) 就是所要求的不超过 $N = 100$ 的素数.

将上述解答列表如下:

对于素数 $p_1 = 2$,

1	2	3	~~4~~	5	~~6~~	7	~~8~~	9	~~10~~
11	~~12~~	13	~~14~~	15	~~16~~	17	~~18~~	19	~~20~~
21	~~22~~	23	~~24~~	25	~~26~~	27	~~28~~	29	~~30~~
31	~~32~~	33	~~34~~	35	~~36~~	37	~~38~~	39	~~40~~
41	~~42~~	43	~~44~~	45	~~46~~	47	~~48~~	49	~~50~~
51	~~52~~	53	~~54~~	55	~~56~~	57	~~58~~	59	~~60~~
61	~~62~~	63	~~64~~	65	~~66~~	67	~~68~~	69	~~70~~
71	~~72~~	73	~~74~~	75	~~76~~	77	~~78~~	79	~~80~~
81	~~82~~	83	~~84~~	85	~~86~~	87	~~88~~	89	~~90~~
91	~~92~~	93	~~94~~	95	~~96~~	97	~~98~~	99	~~100~~

对于素数 $p_2 = 3$,

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

对于素数 $p_3 = 5$,

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

对于素数 $p_4 = 7$,

1	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47		~~49~~	
		53						59	
61						67			
71		73				~~77~~		79	
		83						89	
~~91~~						97			

余下的整数 (不包括 1) 就是所要求的不超过 $N = 100$ 的素数.

~~1~~	2	3		5		7			
11		13				17		19	
		23						29	
31						37			
41		43				47			
		53						59	
61						67			
71		73						79	
		83						89	
						97			

即 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.

下面证明素数有无穷多个.

定理 1.1.8 *素数有无穷多个.*

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

$$n = p_1 \cdot p_2 \cdots p_k + 1.$$

因为 $n > p_i,\quad i = 1, \cdots, k$, 所以 n 一定是合数. 根据定理 1.1.6, n 的大于 1 的最小正因数 p 是素数. 因此, p 是 $p_1,\ p_2,\ \cdots,\ p_k$ 中的某一个, 即存在 $j,\ 1 \leqslant j \leqslant k$, 使得 $p = p_j$. 根据定理 1.1.3, 有

$$p \mid n - (p_1 \cdots p_{j-1} \cdot p_{j+1} \cdots p_k) \cdot p_j = 1.$$

这是不可能的. 故存在无穷多个素数. 证毕.

1.1.3 欧几里得除法 —— 最小非负余数

因为不是任意两个整数之间都有整除关系的, 所以这里引进欧几里得 (Euclid) 除法或带余数除法.

定理 1.1.9 (欧几里得除法) *设 $a,\ b$ 是两个整数, 其中 $b > 0$, 则存在唯一的整数 $q,\ r$ 使得*

$$a = q \cdot b + r, \quad 0 \leqslant r < b. \tag{1.2}$$

定理 1.1.9 的证明: (存在性) 考虑一个整数序列

$$\cdots,\ -3 \cdot b,\ -2 \cdot b,\ -b,\ 0,\ b,\ 2 \cdot b,\ 3 \cdot b,\ \cdots$$

它们将实数轴分成长度为 b 的区间, 而 a 必定落在其中的一个区间中. 因此存在一个整数 q 使得

$$q \cdot b \leqslant a < (q+1) \cdot b.$$

令 $r = a - q \cdot b$, 则有

$$a = q \cdot b + r, \quad 0 \leqslant r < b.$$

(唯一性) 如果分别有整数 $q,\ r$ 和 $q_1,\ r_1$ 满足式 (1.2), 则

$$\begin{aligned} a &= q \cdot b + r, \quad 0 \leqslant r < b, \\ a &= q_1 \cdot b + r_1, \quad 0 \leqslant r_1 < b. \end{aligned}$$

两式相减, 有

$$(q - q_1) \cdot b = -(r - r_1).$$

当 $q \neq q_1$ 时, 左边的绝对值 $\geqslant b$, 而右边的绝对值 $< b$, 这是不可能的, 故 $q = q_1,\ \ r = r_1$.

证毕.

定义 1.1.3 *式 (1.2) 中的 q 叫做 a 被 b 除所得的*不完全商*, r 叫做 a 被 b 除所得的*余数*.*

推论 在定理 1.1.9 的条件下, $b \mid a$ 的充要条件是 a 被 b 除所得的余数 $r = 0$.

为了更好地描述不完全商和余数, 且表述一些数学概念和问题, 下面引进一个数学符号.

定义 1.1.4 设 x 是实数. 称 x 的整数部分为小于或等于 x 的最大整数, 记成 $[x]$. 这时, 有

$$[x] \leqslant x < [x] + 1.$$

注 定理 1.1.9 中的不完全商 q 可写为 $q = \left[\dfrac{a}{b}\right]$, 余数 r 可写为 $r = a - q \cdot b = a - \left[\dfrac{a}{b}\right] \cdot b$. 事实上, 也是先计算不完全商 $q = \left[\dfrac{a}{b}\right]$, 再计算余数 $r = a - q \cdot b = a - \left[\dfrac{a}{b}\right] \cdot b$ 的.

例 1.1.10 $[3.14] = 3,\ [-3.14] = -4,\ [3] = 3,\ [-3] = -3.$

例 1.1.11 设 $b = 15$.

当 $a = 255$ 时,

$$a = 17 \cdot b + 0, \quad q = \left[\frac{255}{15}\right] = 17,\ r = 255 - 17 \cdot 15 = 0 < 15;$$

当 $a = 417$ 时,

$$a = 27 \cdot b + 12, \quad q = \left[\frac{417}{15}\right] = 27,\ 0 < r = 417 - 27 \cdot 15 = 12 < 15;$$

当 $a = -81$ 时,

$$a = -6 \cdot b + 9, \quad q = \left[\frac{-81}{15}\right] = -6,\ 0 < r = -81 - (-6) \cdot 15 = 9 < 15.$$

1.1.4 素数的平凡判别

应用定理 1.1.7 和欧几里得除法, 可以具体判断一个整数是否为素数 (用到整数的乘法和加法运算).

素数的平凡判别. 对于给定正整数 N, 设不大于 $\sqrt{N}$ 的所有素数为 $p_1,\ p_2,\ \cdots, p_s$. 如果 N 被所有 p_i 除的余数都不为零, 即 $p_i \nmid n,\ \ 1 \leqslant i \leqslant s$, 则 N 是素数.

例 1.1.12 证明 $N = 137$ 为素数.

解 因为 $N = 137$, 不大于 $\sqrt{N} < 12$ 的所有素数为 2, 3, 5, 7, 11, 所以依次用 2, 3, 5, 7, 11 去试除.

$$137 = 68 \cdot 2 + 1, \qquad 137 = 45 \cdot 3 + 2, \qquad 137 = 27 \cdot 5 + 2,$$
$$137 = 19 \cdot 7 + 4, \qquad 137 = 12 \cdot 11 + 5.$$

根据定理 1.1.9 的推论, 有 $2 \nmid 137,\ 3 \nmid 137,\ 5 \nmid 137,\ 7 \nmid 137,\ 11 \nmid 137$. 根据定理 1.1.7, $N = 137$ 为素数. 证毕.

1.1.5 欧几里得除法 —— 一般余数

实际运用欧几里得除法时, 可以根据需要将余数取成其他形式.

定理 1.1.10 (**欧几里得除法**) 设 $a,\ b$ 是两个整数, 其中 $b > 0$. 则对任意的整数 c, 存在唯一的整数 $q,\ r$ 使得

$$a = q \cdot b + r, \quad c \leqslant r < b + c. \tag{1.3}$$

定理 1.1.10 的证明: (存在性) 考虑一个整数序列

$$\cdots,\ -3 \cdot b + c,\ -2 \cdot b + c,\ -b + c,\ c,\ b + c,\ 2 \cdot b + c,\ 3 \cdot b + c,\ \cdots$$

它们将实数轴分成长度为 b 的区间, 而 a 必定落在其中的一个区间中. 因此存在一个整数 q 使得

$$q\cdot b+c\leqslant a<(q+1)\cdot b+c.$$

令 $r=a-q\cdot b$, 则有

$$a=q\cdot b+r,\quad c\leqslant r<b+c.$$

(唯一性) 如果分别有整数 q, r 和 q_1, r_1 满足式 (1.3), 则

$$\begin{aligned} a &= q\cdot b + r, \quad c\leqslant r<b+c,\\ a &= q_1\cdot b + r_1, \quad c\leqslant r_1<b+c. \end{aligned}$$

两式相减, 有

$$(q-q_1)\cdot b=-(r-r_1).$$

当 $q\neq q_1$ 时, 左边的绝对值 $\geqslant b$, 而右边的绝对值 $<b$, 这是不可能的, 故 $q=q_1,\ \ r=r_1$.

证毕.

注 实际运用欧几里得除法和余数 ($c\leqslant r\leqslant b+c-1$) 时, 常采用以下形式的余数.

(1) 当 $c=0$ 时, 有 $b+c=b$ 及 $0\leqslant r\leqslant b-1<b$. 这时 r 叫做**最小非负余数**.

(2) 当 $c=1$ 时, 有 $b+c=b+1$ 及 $1\leqslant r\leqslant b$. 这时 r 叫做**最小正余数**.

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

(4) 当 $c=-b$ 时, 有 $b+c=0$ 及 $-b\leqslant r\leqslant -1<0$, 这时 r 叫做**最大负余数**.

(5) ①当 b 为偶数, $c=-\dfrac{b}{2}$ 时, 有 $b+c=\dfrac{b}{2}$ 及 $-\dfrac{b}{2}\leqslant r\leqslant \dfrac{b-2}{2}<\dfrac{b}{2}$;

②当 b 为偶数, $c=-\dfrac{b-2}{2}$ 时, 有 $b+c=\dfrac{b+2}{2}$ 及 $-\dfrac{b}{2}<-\dfrac{b-2}{2}\leqslant r\leqslant \dfrac{b}{2}$;

③当 b 为奇数, $c=-\dfrac{b-1}{2}$ 时, 有 $b+c=\dfrac{b+1}{2}$ 及 $-\dfrac{b}{2}<-\dfrac{b-1}{2}\leqslant r\leqslant \dfrac{b-1}{2}<\dfrac{b}{2}$.

总之, 有

$$-\frac{b}{2}\leqslant r<\frac{b}{2}\qquad 或\qquad -\frac{b}{2}<r\leqslant\frac{b}{2}.$$

这时, r 叫做**绝对值最小余数**.

例 1.1.13 设 $b=7$, 则

余数 $r=0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6$ 为最小非负余数.

余数 $r=1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7$ 为最小正余数.

余数 $r=0,\ -1,\ -2,\ -3,\ -4,\ -5,\ -6$ 为最大非正余数.

余数 $r=-1,\ -2,\ -3,\ -4,\ -5,\ -6,\ -7$ 为最大负余数.

余数 $r=-3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3$ 为绝对值最小余数.

例 1.1.14 设 $b=8$, 则

余数 $r=0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7$ 为最小非负余数.

余数 $r=1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8$ 为最小正余数.

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

余数 $r=-1,\ -2,\ -3,\ -4,\ -5,\ -6,\ -7,\ -8$ 为最大负余数.

余数 $r=-4.\ -3,\ -2,\ -1,\ 0,\ -1,\ -2,\ -3$

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

1.2 整数的表示

1.2.1 b 进制

平时遇到的整数通常是以十进制表示的. 例如 51 328 意指

$$5\cdot 10^4+1\cdot 10^3+3\cdot 10^2+2\cdot 10^1+8\cdot 10^0.$$

中国是世界上最早采用十进制的国家, 春秋战国时期已普遍使用的算筹就严格遵循十进位制, 见《孙子算经》. 但在计算机中, 51 328 要用二进制, 八进制或十六进制表示. 为此, 考虑一般的 b 进制, 再考查特殊的二进制, 十进制和十六进制. 运用欧几里得除法, 可得到以下定理.

定理 1.2.1 设 b 是大于 1 正整数, 则每个正整数 n 可唯一地表示成

$$n=a_{k-1}\,b^{k-1}+a_{k-2}\,b^{k-2}+\cdots+a_1\,b+a_0, \tag{1.4}$$

其中 a_i 是整数, $0\leqslant a_i\leqslant b-1,\ i=1,\cdots,k-1$, 且首项系数 $a_{k-1}\neq 0$.

证 先证明 n 有表达式. 具体方法是逐次运用欧几里得除法, 以得到所期望的表示式.

首先, 用 b 去除 n 得到

$$n=q_0b+a_0,\quad 0\leqslant a_0\leqslant b-1.$$

再用 b 去除不完全商 q_0 得到

$$q_0=q_1b+a_1,\quad 0\leqslant a_1\leqslant b-1.$$

继续这类算法, 依次得到

$$\begin{aligned}
q_1 &= q_2b + a_2, && 0\leqslant a_2\leqslant b-1,\\
q_2 &= q_3b + a_3, && 0\leqslant a_3\leqslant b-1,\\
&\vdots &&\\
q_{k-3} &= q_{k-2}b + a_{k-2}, && 0\leqslant a_{k-2}\leqslant b-1,\\
q_{k-2} &= q_{k-1}b + a_{k-1}, && 0\leqslant a_{k-1}\leqslant b-1.
\end{aligned}$$

因为

$$0\leqslant q_{k-1}<q_{k-2}<\cdots<q_2<q_1<q_0<n,$$

所以必有整数 k 使得不完全商 $q_{k-1}=0$.

这样, 依次得到

$$\begin{aligned}
n &= q_0b+a_0,\\
n &= (q_1b+a_1)b+a_0=q_1b^2+a_1b+a_0,\\
&\vdots\\
n &= q_{k-3}b^{k-2}+a_{k-3}b^{k-3}+\cdots+a_1b+a_0,
\end{aligned}$$

$$\begin{aligned} n &= q_{k-2}b^{k-1} + a_{k-2}b^{k-2} + \cdots + a_1 b + a_0, \\ &= (q_{k-1}b + a_{k-1})b^{k-1} + a_{k-2}b^{k-2} + \cdots + a_1 b + a_0, \\ &= a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \cdots + a_1 b + a_0. \end{aligned}$$

再证明这个表示式 (1.4) 是唯一的. 如果有两种不同的表示式:

$$n = a_{k-1}b^{k-1} + a_{k-2}b^{k-2} + \cdots + a_1 b + a_0, \quad 0 \leqslant a_i \leqslant b-1,\ i = 1, \cdots, k-1.$$

$$n = c_{k-1}b^{k-1} + c_{k-2}b^{k-2} + \cdots + c_1 b + c_0, \quad 0 \leqslant c_i \leqslant b-1,\ i = 1, \cdots, k-1.$$

(这里可以取 $a_{k-1} = 0$ 或 $c_{k-1} = 0$.) 两式相减得到

$$(a_{k-1} - c_{k-1})b^{k-1} + (a_{k-2} - c_{k-2})b^{k-2} + \cdots + (a_1 - c_1)b + (a_0 - c_0) = 0.$$

假设 j 是最小的正整数使得 $a_j \neq c_j$, 则

$$\left((a_{k-1} - c_{k-1})b^{k-1-j} + (a_{k-2} - c_{k-2})b^{k-2-j} + \cdots + (a_{j+1} - c_{j+1})b + (a_j - c_j)\right) b^j = 0.$$

或者

$$(a_{k-1} - c_{k-1})b^{k-1-j} + (a_{k-2} - c_{k-2})b^{k-2-j} + \cdots + (a_{j+1} - c_{j+1})b + (a_j - c_j) = 0.$$

因此

$$a_j - c_j = -\left((a_{k-1} - c_{k-1})b^{k-j-2} + (a_{k-2} - c_{k-2})b^{k-j-3} + \cdots + (a_{j+1} - c_{j+1})\right) b.$$

故

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

但

$$0 \leqslant a_j \leqslant b-1, \quad 0 \leqslant c_j \leqslant b-1,$$

又有 $|a_j - c_j| < b$, 这不可能, 也就是说 n 的表示式是唯一的. 证毕.

为了说明关于基 b 的整数表示式, 引进以下符号.

定义 1.2.1 用

$$n = (a_{k-1}a_{k-2}\cdots a_1 a_0)_b, \tag{1.5}$$

表示展开式 (1.4) 得

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

其中 $0 \leqslant a_i \leqslant b-1,\ i = 1, \cdots, k-1,\ a_{k-1} \neq 0$, 并称其为整数 n 的 b **进制表示**. 这时, n 的 b 进制位数是 $k = [\log_b n] + 1$. 事实上,

$$b^{k-1} \leqslant n < b^k \quad \text{或} \quad k - 1 \leqslant \log_b n < k.$$

因此, $k - 1 = [\log_b n]$.

当 $b = 2$, 系数 a_i 为 0 或 1, 因此有推论:

推论 每个正整数都可以表示成不同的 2 的幂的和.