第一章 整数的可除性
2020年02月25日

信息安全数学基础

陈恭亮　教授 博士生导师

上海交通大学网络空间安全学院

chengl@sjtu.edu.cn

本章主要思考的一些问题

1. 整数集合**Z** 中的整数, 对于乘法运算, 其极小整数(不能分解为两个更小整数的乘积)是什么? 这样的极小整数是唯一的吗? 用何种表示可说明它们的唯一性?
2. 如何判断一个正整数为素数. 编成实现厄拉托塞师筛法的算法, 可求出10000 以内的全部素数.
3. 编成实现欧几里得除法(定理1.1.9), 并可判断整数a 是否被非零整数整除.
4. 编成实现应用平凡除法判断一个整数(定理1.1.7) 是否为素数的算法, 可判断出100000 以内的整数是否为素数.
5. 如何求两个整数的公因数及最大公因数. 编成实现求两个整数的最大公因数(定理1.3.4) 的算法, 可计算出100000 以内的两个整数的最大公因数.
6. 对给定正整数m, 编成实现判断整数a 是否与m 互素的算法.
7. 编成实现计算Bézout (贝祖)等式的算法(定理1.3.7). 即对于两个正整数a, b, 可计算出整数s, t 使得(3.16) 成立: $s \cdot a + t \cdot b = (a, b)$.

本章主要讲述如下问题

1. 整除的定义、可否推广到多项式、矩阵、整环
2. 素数 乘法的最小单位
3. 若 $c \mid a \cdot b$, 则 $c \mid a$ 或 $c \mid b$.
3. 若 $p \mid a \cdot b$, 则 $p \mid a$ 或 $p \mid b$.
4. 如何找素数
5. 厄拉托塞师(Eratosthenes) 筛法
6. 欧几里得除法 不完全商 余数
7. 最大公因数
8. 广义欧几里得除法

本章主要讲述如下问题

1. 整除 因数 倍数
2. 素数 合数
3. 厄拉托塞师(Eratosthenes) 筛法
4. 欧几里得除法 不完全商 余数
5. 整数的b-进制表示
6. 最大公因数
7. 广义欧几里得除法
8. 整数的性质 最小公倍数
9. 算术基本定理
10. 素数定理

1.1.1 整除的概念

本节考虑关于整数的基本概念和性质: 整除和欧几里得除法.

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

$$a = q \cdot b. \tag{1}$$

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**. 这时, q 也是a 的因数, 常将q 写成a/b 或$\frac{a}{b}$.
否则, 就称b 不能整除a 或者a 不能被b 整除,记作$b \nmid a$.

注1 整除定义1.1.1 仅与乘法运算相关, 与小学整除定义有极大区别.

注2 本整除定义1.1.1 可推广为现代数学的整除定义.

注3 当b 遍历整数a 的所有因数时, $-b$ 遍历整数a 的所有因数.

注4 当b 遍历整数a 的所有因数时, $\frac{a}{b}$ 遍历整数a 的所有因数.

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

有$2,\ 3,\ 5$ 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.

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

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

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

* 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,

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

因为$-q$, q 都是整数, 根据整除的定义, 有

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

定理1.1.1 设a, $b \neq 0$, $c \neq 0$是整数. 若 $c \mid b$, $b \mid a$, 则 $c \mid a$.(传递性)

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

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

因此, 我们有 $\quad a = q_1 \cdot b = q_1(q_2 \cdot c) = q \cdot c.$

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

注 数学证明的表述.

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

定理1.1.2 设$a, b, c \neq 0$是整数. 若$c \mid a, c \mid b$, 则$c \mid a \pm b$.(**加法运算**)

证 设$c \mid a, c \mid b$, 那么存在整数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.

例4 因为$7 \mid 14, 7 \mid 84$, 所以

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

定理1.1.3 设$a, b, c \neq 0$是整数. 若$c \mid a, c \mid b$, 则对任意整数s, t, 有

$c \mid s \cdot a + t \cdot b.$ (**整系数线性组合**)

证 设$c|a, c|b$, 那么存在整数q_1, q_2 分别使得

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

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

例1.1.5 因为$7|14,\ 7|21$,故

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

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

证 设$c\mid a\cdot n,\ c\mid b\cdot n$, 因为存在整数$s,\ t$, 使得$s\cdot a+t\cdot b=1$, 根据定理3, 有

$$c\mid s(a\cdot n)+t(b\cdot n)=(s\cdot a+t\cdot b)n=n.$$

因此, $c\mid n$.

定理1.1.3 可推广为:

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

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

是c 的倍数.

例1.1.7 因为$7|14,\ 7|21,\ 7|35$, 所以

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

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,

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

这样, $q_1\cdot q_2=1$. (为什么?)
因为$q_1,\ q_2$ 是整数, 所以$q_1=q_2=\pm 1$. 进而, $a=\pm b$.

素数

前面考虑了整除和因数, 现考虑不能继续分解的整数. 更确切地说是关于乘法运算的整数最小元素.

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 没有其它因数, 则n 叫做**素数** (或**质数** 或**不可约数**).
否则, n 叫做**合数**.

因n 和$-n$ 同为素数或合数, 故约定素数总是指正整数, 通常写成p.

例1.1.8 整数 $2, \ 3, \ 5, \ 7$ 都是素数; 整数$4, \ 10, \ 21, \ 30$ 都是合数.
因为$4 = 2 \cdot 2, \ 10 = 2 \cdot 5, \ 21 = 3 \cdot 7,$
$30 = 2 \cdot 15 = 3 \cdot 10 = 5 \cdot 6.$

下面证明素数的存在性, 即每个合数必有素因子.

最小的非单位元为素数(乘法).

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$p \leq \sqrt{n}$.

证 反证法. 若p 不是素数, 则存在q, $1 < q < p$, 使得

$$q \mid p. \quad 但 \quad p \mid n,$$

由定理1.1.1, 有

$$q \mid n.$$

这与p 是最小正因数矛盾. 故p 是素数.

因为n 是合数, 所以

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

因此,

$$p^2 \leq n, \qquad p \leq \sqrt{n}.$$

证毕

1.1.2 厄拉托塞师(Eratosthenes) 筛法

根据定理1.1.6, 立即得到一个整数为素数的判别法则.

定理1.1.7 设$n > 1$. 若对所有的素数 $p \le \sqrt{n}$, 有$p \nmid n$, 则n 是素数.

* 应用定理1.1.7, 我们有一个寻找素数的确定性方法, 通常叫做**厄拉托塞师(Eratosthenes) 筛法**.

对任意给定的正整数N , 要求出所有不超过N 的素数. 我们列出N 个整数, 从中删除$\le \sqrt{N}$ 的所有素数$p_1, \ldots, p_k$ 的倍数. 具体地是依次删除,

$$
\begin{array}{ll}
p_1 \text{ 的倍数:} & 2 \cdot p_1, \ \ldots, \ \left[\dfrac{N}{p_1}\right] \cdot p_1; \\
& \quad \cdots\cdots \\
p_k \text{ 的倍数:} & 2 \cdot p_k, \ \ldots, \ \left[\dfrac{N}{p_k}\right] \cdot p_k,
\end{array}
$$

余下的整数(不包括1) 就是所要求的不超过N 的素数.

例1.1.9 求出所有不超过$N = 100$ 的素数.

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

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

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

余下整数(不包括1) 就是所求的不超过$N = 100$ 的素数:

$\cancel{1}$	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.

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$p_1, \ p_2, \ \ldots, \ p_k$. 考虑整数

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

因为$n > p_i, \quad i = 1, \ldots, k$, 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$p_1, \ p_2, \ \ldots, \ p_k$ 中的某一个, 即存在$j, \ 1 \le j \le k$, 使得$p = p_j$. 根据定理3, 我们有

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

这是不可能的. 故存在有无穷多个素数.

运用上述方法可证明形为$4k+3$ 的素数有无穷多个, 但无法证明形为$4k+1$ 的素数有无穷多个. 需要更多技巧.

1.1.3 欧几里得(Euclid)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, 所以我们引进**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$b > 0$. 则存在惟一的整数$q, \ r$ 使得

$$a = q \cdot b + r, \quad 0 \le r < b \tag{2}$$

证: (存在性) 考虑一个整数序列

$$\ldots, \ -3 \cdot b, \ -2 \cdot b, \ -b, \ 0, \ b, \ 2 \cdot b, \ 3 \cdot b, \ \ldots.$$

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

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

我们令$r = a - q \cdot b$, 则有 $\quad a = q \cdot b + r, \quad 0 \le r < b.$

(惟一性) 如果分别有整数 q, r 和 q_1, r_1 满足(2), 则

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

两式相减, 有 $\quad (q - q_1)b = -(r - r_1).$

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

定义1.1.3 (2) 式中的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, $b \mid a \iff r = 0$.

注1 推论表明整除的定义等价于小学的整除定义. 并可用余数$r = 0$ 作为a 被b 整除的判断.

注2 欧几里得除法在密码算法中起着**核心作用**, 其改进关系到密码系统的效率. 如$b = 2^u + v$, v 很小.

如何求q 和r

给定正整数 a, b, 求 q 和 r 使得 $a = q \cdot b + r, \quad 0 \le r < b$?

可以做如下计算

1) 如果$a < b$, 则取 $q = 0,\ r = a$. 否则, 令

$$a_1 = a - b, \quad q_1 = 1.$$

2) 如果$a_1 < b$, 则取 $q = q_1,\ r = a_1$. 否则, 令

$$a_2 = a_1 - b = a - 2 \cdot b, \quad q_2 = q_1 + 1 = 2.$$

如此下去, 存在k 使得

$$0 < a_k = a_{k-1} - b = a - k \cdot b < b, \quad q_k = q_{k-1} + 1 = k.$$

$k+1$) 最后, 取 $q = q_k = k,\ r = a_k$, 有

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

函数$[x]$

为了更好的描述不完全商和余数, 以及今后表述一些数学概念和问题, 我们引进一个数学符号.

定义1.1.4 设x 是一个实数. 我们称x 的整数部分为小于或等于x 的最大整数, 记成$[x]$. 这时, 我们有

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

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

注1 定理1.1.9 中不完全商q 和余数r 可写为

$$q = \left[\frac{a}{b}\right], \qquad r = a - \left[\frac{a}{b}\right] \cdot b.$$

事实上, 由 $a = q \cdot b + r$, 有 $\dfrac{a}{b} = q + \dfrac{r}{b}$.

因此, $q = \left[\dfrac{a}{b}\right]$.

注2 定理1.1.9 中, 先计算不完全商 $q = \left[\frac{a}{b}\right]$,

再计算余数 $r = a - \left[\frac{a}{b}\right] b$.

例1.1.11 设$b = 15$.

当$a = 255$ 时,

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

当$a = 417$ 时,

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

当$a = -81$ 时,

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

整数为素数的确定性检验

应用定理1.1.7和欧几里得除法, 可具体判断一个整数是否为素数.

例1.1.12 证明$N = 137$ 为素数.

解 因为$\le \sqrt{137} < 12$ 的所有素数为

$$2,\ 3,\ 5,\ 7,\ 11,$$

所以依次用$2,\ 3,\ 5,\ 7,\ 11$ 去试除:

$$\begin{aligned}137 &= 68 \cdot 2 + 1,\\ 137 &= 45 \cdot 3 + 2,\\ 137 &= 26 \cdot 5 + 3,\\ 137 &= 19 \cdot 7 + 4,\\ 137 &= 12 \cdot 11 + 5.\end{aligned}$$

因此, $2 \nmid 137,\ 3 \nmid 137,\ 5 \nmid 137,\ 7 \nmid 137,\ 11 \nmid 137.$

由定理1.1.7, $N = 137$ 为素数.

1.1.3 欧几里得(Euclid)除法–一般余数

实际运用欧几里得除法时, 可根据需要将余数取成其它形式.

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, 存在惟一的整数q, r 使得

$$a = q \cdot b + r, \quad c \le r < b + c \tag{3}$$

证: (存在性) 考虑一个整数序列

$$\ldots, \ -3 \cdot b + c, \ -2 \cdot b + c, \ -b + c, \ c, \ b + c, \ 2 \cdot b + c, \ 3 \cdot b + c, \ \ldots.$$

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

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

我们令 $r = a - q \cdot b$, 则有

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

(惟一性) 如果分别有整数q, r 和q_1, r_1 满足(3), 则

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

两式相减, 我们有

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

当$q \neq q_1$时,

$$|(q - q_1)b| \ge b, \qquad | - (r - r_1)| < b.$$

这是不可能的. 故 $q = q_1, \quad r = r_1$.

余数的表示

运用欧几里得除法和余数($c \le r \le b+c-1$)时, 常采用如下形式的余数.

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

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

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

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

5. i) 当b 为偶数, $c=-\frac{b}{2}$ 时, 有$b+c=\frac{b}{2}$ 及 $-\frac{b}{2} \le r \le \frac{b-2}{2} < \frac{b}{2}$,

   ii) 当b 为偶数, $c=-\frac{b-2}{2}$ 时, 有$b+c=\frac{b+2}{2}$ 及 $-\frac{b}{2} < -\frac{b-2}{2} \le r \le \frac{b}{2}$,

   iii) 当b 为奇数, $c=-\frac{b-1}{2}$ 时, 有$b+c=\frac{b+1}{2}$ 及

$$-\frac{b}{2} < -\frac{b-1}{2} \le r \le \frac{b-1}{2} < \frac{b}{2}.$$

总之, 我们有

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

这时, r 叫做**绝对值最小余数**.

访问主页
标题页
目录页
第 27 页 共 29 页
返回
全屏显示
关闭
退出

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.

作业2020-02-25

1. 补充定理1.1.4 之证明:

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

2. (习题1.8 (13)) 证明: $4k+3$ 形式的素数有无穷多个.

3. (习题1.8 (20)) 证明: 当$n = 0, 1, 2, \cdots, 39$时, 整数n^2+n+41 都是素数.

4. (习题1.8 (21)) 证明: 当$n > 1$ 时, $1 + \frac{1}{2} + \cdots + \frac{1}{n}$ 不是整数.

思考题:

1. (思考1.8 (1)) 整数集合**Z** 中的整数, 对于乘法运算, 其极小整数(不能分解为两个更小整数的乘积)是什么? 这样的极小整数是唯一的吗? 用何种表示可说明它们的唯一性?

2. (思考1.8 (2)) 如何判断一个正整数为素数. 编成实现厄拉托塞师筛法的算法, 可求出10000 以内的全部素数.

3. (思考1.8 (3)) 编成实现欧几里得除法, 并可判断整数a 是否被非零整数整除.

4. (思考1.8 (4)) 编成实现应用平凡除法判断一个整数是否为素数的算法, 可判断出100000 以内的整数是否为素数.