

大 学

数学系

697387

315

4660

T. 1

自学丛书

高等代数

上册



GAO DENG DAISHU

697387

315

4660

T. 1

大学数学系自学丛书

高等代数

上册

东北师范大学

贺昌亭 主编

辽宁人民出版社

一九八三年·沈阳

责任编辑：于 乞

封面设计：安今生

大学数学系自学丛书

高等代数

(上)

贺昌亭 主编

·
辽宁人民出版社出版

(沈阳市南京街6段1里2号)

辽宁省新华书店发行

朝阳六六七厂印刷

·
开本：850×1168^{1/2} 印张：15

字数：396,000 印数：1—16,200

1983年6月第1版 1983年6月第1次印刷

统一书号：7090·226 定价：1.90 元

目 录

第一章 数的基础知识……(1)	§ 7 方程及其变 换……………(65)
§ 1 自然数与数 学归纳法……(3)	§ 8 复系数多项 式……………(72)
§ 2 整数的整除 性……………(8)	§ 9 实系数多项 式……………(76)
§ 3 因数分解定 理……………(16)	§ 10 有理系数多 项式……………(85)
§ 4 数域……………(20)	§ 11 部分分式……(95)
习题一……………(24)	习题二……………(100)
第二章 一元多项式……(26)	第三章 多元多项式……(102)
§ 1 一元多项式的 定义及运算……(26)	§ 1 多元多项式的 定义及运算……(102)
§ 2 多项式的整除性 ——因式、公因式、最高 公因式 ……………(30)	§ 2 对称多项式……(108)
§ 3 带余除法 辗转相除法……(35)	§ 3 分母有理化……(117)
§ 4 多项式的因式 分解……………(46)	习题三……………(123)
§ 5 重因式……(51)	第四章 消元法……………(125)
§ 6 多项式的根……(58)	§ 1 线性方程组的 同解……………(125)
	§ 2 线性方程组的 一种解法—— 消元法……………(130)

§ 3	矩阵在初等变换下的标准形……………(150)	础解系……………(248)
	习题四……………(158)	习题六……………(276)
第五章	行列式……………(161)	学习指导
§ 1	二、三阶行列式……………(162)	第一章 数的基础知
§ 2	排列的奇偶性……………(170)	识……………(281)
§ 3	n 阶行列式……………(176)	[内容提要]……………(281)
§ 4	行列式的性质和计算……………(187)	[内容分析]……………(282)
§ 5	矩阵的秩……………(212)	[例题选解]……………(286)
	习题五……………(222)	第二章 一元多项式……………(289)
第六章	线性方程组的理论……………(226)	[内容提要]……………(289)
§ 1	线性方程组的有解条件……………(226)	[内容分析]……………(290)
§ 2	线性方程组的公式解——克莱姆(Cramer)法则……………(234)	[例题选解]……………(301)
§ 3	线性方程组解之间的关系……………(244)	第三章 多元多项式……………(318)
§ 4	n 维向量的线性相关性及其基	[内容提要]……………(318)
		[内容分析]……………(319)
		[例题选解]……………(325)
		第四章 消元法……………(332)
		[内容提要]……………(332)
		[内容分析]……………(335)
		[例题选解]……………(350)
		第五章 行列式……………(354)
		[内容提要]……………(354)
		[内容分析]……………(357)
		[例题选解]……………(366)
		第六章 线性方程组的理论……………(378)

〔内容提要〕……………(378)	练习二……………(426)
〔内容分析〕……………(381)	练习三……………(427)
〔例题选解〕……………(394)	习题三……………(428)
练习与习题解答	
第一章 数的基础	第四章 消元法 ……………(433)
知识……………(403)	练习一……………(433)
练习一……………(403)	练习二……………(433)
练习二……………(405)	练习三……………(435)
练习三……………(405)	习题四……………(437)
练习四……………(407)	第五章 行列式 ……………(445)
习题一……………(408)	练习一……………(445)
第二章 一元多项式 ……………(413)	练习二……………(445)
练习一……………(413)	练习三……………(447)
练习二……………(413)	练习四……………(449)
练习三……………(414)	练习五……………(452)
练习四……………(415)	习题五……………(452)
练习五……………(415)	第六章 线性方程组的理
练习六……………(416)	论……………(456)
练习七……………(416)	练习一……………(456)
练习九……………(417)	练习二……………(458)
练习十……………(417)	练习四……………(460)
练习十一……………(418)	习题六……………(462)
习题二……………(419)	附录 关于连加号
第三章 多元多项式 ……………(426)	“ Σ ” ……(469)
练习一……………(426)	

第一章 数的基础知识

本章把以下要用到的有关数的一些基本性质集中起来讲三个问题：

1. 自然数与数学归纳法；
2. 整数的整除性；
3. 数域。

这些内容在中学数学里大部分都已讲过，因此这里主要目的是集中复习一下这些知识，以便下面引用。

为了以下说和写的方便，我们先介绍几个数学用语及符号。

集合

随便一些对象(事物)做为整体,叫做一个集合。特别地,以数为对象组成的集合简称为数集。以下常用大写的拉丁字母表示集合。

例如,一切正整数的整体组成一个数集,叫做自然数集,记作 $N = \{1, 2, 3, \dots\}$ 或 $N: 1, 2, 3, \dots$ 。

一切整数也组成一个数集,叫整数集。通常用 Z 表示整数集,即记作

$$Z = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$$

或

$$Z: \dots, -3, -2, -1, 0, 1, 2, 3, \dots$$

而集合

$A: ax^2 + bx + c = 0$; 其中 a, b, c 为任意实数,且 $a \neq 0$, 是由一切实系数一元二次方程为对象组成的。

$B: (x, 0)$; x 为任意实数,

这个集合 B 就是平面上给定笛卡儿直角坐标系之后,以横坐标轴上

的点为对象组成的。

元素

设 X 为任一集合。组成集合 X 的每一个对象都叫做 X 的一个元素。一般用小写的拉丁字母表示元素。如果 x 是 X 的一个元素，则称 x 属于 X 或说 X 含有 x ，记作 $x \in X$ 。如果 x 不是 X 的一个元素，则称 x 不属于 X 或说 X 不含有 x ，记作 $x \notin X$ 。

例如，正整数 $1, 2, 3$ 都属于自然数集 N ，即 $1 \in N, 2 \in N, 3 \in N$ ，而 N 不含有 $-1, 0$ ，所以 $-1 \notin N, 0 \notin N$ 。类似地，一元二次方程 $x^2 + 2x + 1 = 0$ 与 $x^2 - 1 = 0$ 都是集合 A 的元素，所以 $x^2 + 2x + 1 = 0 \in A, x^2 - 1 = 0 \in A$ ；但 $x - 1 = 0 \notin A$ ，因为 A 不含有一次方程。再有我们用倒写的 A 表示“任意的”意思，比如，“ a 是自然数集 N 的任意一个自然数”这句话的内容便可记作： $\forall a \in N$ 。

相等

设 X, Y 为任二集合。如果 X 与 Y 是由完全相同的元素组成的，即凡属于 X 的元素都属于 Y ，同时凡属于 Y 的元素也都属于 X ，则称 X 与 Y 是相同的集合，也叫 X 与 Y 相等，记作 $X = Y$ 。例如

$$X = \{1, -1\},$$

$$Y = \{k \mid k \text{ 是 } x^2 - 1 = 0 \text{ 的根}\}^*$$

这里 X 是由 $1, -1$ 两个数组成的数集， Y 是以方程 $x^2 - 1 = 0$ 的根为元素组成的集合，而 $x^2 - 1 = 0$ 恰有两个根： $1, -1$ ，所以 Y 的元素也是 1 与 -1 这两个数。于是 X 与 Y 是相同的集合，即 $X = Y$ 。

子集

如果集合 X 的元素都属于集合 Y ，则称 X 是 Y 的一个子集，记作 $X \subseteq Y$ ，当 $X \subseteq Y$ 但 $X \neq Y$ 时就说 X 是 Y 的真子集，记作 $X \subset Y$ 。例如 N 是 Z 的一个子集而且是真子集，所以 $N \subset Z$ 。再如用 Q, D, C 分别表示有理数集、实数集和复数集时，于是

$$Q \subseteq D \subseteq C \text{ 且 } Q \subset D \subset C.$$

* 我们常用这样的符号表示集合，即在花括号中划一竖线，竖线前边的字母表示该集合的元素，竖线后边标出这些元素所应满足的条件。

空集

有时做为集合来考虑的整体，当中不含有任何元素，例如

$$X = \{k | k \text{ 为 } x^2 + 1 = 0 \text{ 的实根}\}.$$

因为一元二次方程 $x^2 + 1 = 0$ 没有实根，所以集合 X 不含有任何元素。尽管这样，把不含有任何对象的整体也叫做集合是方便的。今后称不含有任何对象的整体叫空集，记作 ϕ ，并且我们认为空集是任一集合 X 的子集，即 $\phi \subseteq X$ 。

§ 1 自然数与数学归纳法

人们在长期的实践中从数数逐渐认识了自然数及其基本性质。所谓自然数就是

$$1, 2, 3, \dots, n, \dots \quad (1)$$

这些数。如前所述通常用 N 表示一切自然数组成的数集。

大家已经知道自然数集 N 的以下三方面的基本性质：

(I) 自然数集 N 可以进行加法、乘法运算，即任意两个自然数相加的和是自然数，相乘的积也是自然数。例如

$$1+1=2, 2+1=3, 2 \cdot 3=6, 1 \cdot 4=4 \text{ 等等,}$$

特别地，任意一个自然数 m 都可以由 1 自身相加得出来，

$$m = \overbrace{1+1+\dots+1}^{m \text{ 个}}.$$

(II) 自然数之间有大小关系，象 (1) 那样写出一切自然数时，恰好是从左往右由小到大的把自然数列举出来了，即

$$1 < 2 < 3 < \dots < n < \dots.$$

一般说来，对任二自然数 a, b 那么 $a < b$ 当且仅当有自然数 c ，使 $b = a + c$ 。特别地，若 $b = a + 1$ ，则 $a < b$ ，这时就说 a 与 b 是相邻的， b 叫做 a 的“紧后边的”数，也说 b 是 a 的后继数。

1 是自然数集 N 中最小的数，即对任何自然数 n ，如果 $n \neq 1$ 那么 $1 < n$ 。

(Ⅱ) 自然数集 N 的形成规律利用加法可以表述如下:

1 是自然数, 1 加 1 得 2 是自然数, 2 加 1 得 3 是自然数, 如此累次加 1 就得到了全体自然数。换句话说: 1 是自然数从 1 起始累次加 1 就得到了全体自然数。自然数集的这种构成性质是很朴素的, 也很容易被人们所理解, 它正是人们数数过程的数学概括。

我们并不满足于自然数集构成性质的这种朴素的表述。其中累次加 1 是一个无止境的过程, 这当然是由事物的无限性所决定的。但是这种无限过程只不过是“加 1”这种同一方式的无限重复而已。因此我们有可能把这种同一方式的无限重复过程精练归纳为一次完成的递推过程。这样, 对自然数的构成性质我们就又有一种精化了的表述。

第一归纳原理 设 M 是自然数集 N 的一个子集。如果 M 具有以下两条性质:

1. 1 在 M 里;
2. 若 k 在 M 里则 $k+1$ 也在 M 里, 那么一切自然数都在 M 里。

归纳原理是人们对自然数集构成性质认识的深化和精化, 其重要意义在于它给我们提供一种进行数学证明的方法——数学归纳法。

我们用例子来说明用数学归纳法做证明的方法。

例 1 证明: 前 n 个正奇数的和等于 n^2 , 即

$$1+3+5+\cdots+(2n-1)=n^2. \quad (2)$$

这是一个与自然数有关的命题, 要证明的是(2)式对一切自然数 n 都成立。可是自然数有无穷多个, 用有限的时间不可能进行无限次的验证。自然数集的第一归纳原理为解决这个有限与无限的矛盾提供了有力的方法, 即数学归纳法。

为了证明(2)式对一切自然数 n 都成立, 我们用 M 表示使(2)式成立的自然数组成的数集。换句话说, 自然数 k 在 M 里当且仅当 $n=k$ 时(2)式成立。于是(2)式对一切自然数 n 都成立

当且仅当 M 含有一切自然数，即 $M = N$ 。这样，根据第一归纳原理，我们可以分两步验证 $M = N$ ：

- 1) 1 在 M 里，即当 $n = 1$ 时 (2) 式成立；
- 2) 若 k 在 M 里则 $k + 1$ 也在 M 里，即假设 $n = k$ 时 (2) 式成立可以推出 $n = k + 1$ 时 (2) 式也成立。如此便得 $M = N$ 。

事实上

1) 当 $n = 1$ 时 (2) 式左端 = 1，右端 = $1^2 = 1$ ，所以 (2) 式成立，即 1 在 M 里。

- 2) 假设 $n = k$ 时 (2) 式成立。我们看 $n = k + 1$ 的情形，则有
- $$\begin{aligned} & 1 + 3 + \cdots + (2k - 1) + (2k + 1) \\ &= [1 + 3 + \cdots + (2k - 1)] + (2k + 1) \\ &= k^2 + (2k + 1) \\ &= (k + 1)^2. \end{aligned}$$

因此当 $n = k + 1$ 时 (2) 式也成立，即若 k 在 M 里时 $k + 1$ 也在 M 里。这样根据第一归纳原理，便得 $M = N$ ，即 (2) 式对一切自然数 n 都成立。

把上述论证方法概括一下就是有名的数学证明方法——第一数学归纳法：

设 $P(n)$ 是与一切自然数有关的命题。如果

- 1) 当 $n = 1$ 时命题 $P(1)$ 成立；
- 2) 假设 $n = k$ 时命题 $P(k)$ 成立，可推出 $n = k + 1$ 时命题 $P(k + 1)$ 也成立，那么命题 $P(n)$ 对一切自然数 n 都成立。

为了说话方便，我们把 1) 叫递推起点，2) 叫递推过程，2) 中的假设叫做归纳假设。

例 2 证明：对一切自然数 n

$$2 + 4 + 6 + \cdots + 2n = n(n + 1) \quad (3)$$

都成立。

证 用第一数学归纳法，步骤如下：

1) 当 $n=1$ 时, (3) 式左端 = 2, 右端 = $1 \cdot (1+1) = 2$, 所以 (3) 式成立;

2) 假设 $n=k$ 时 (3) 式成立, 看 $n=k+1$ 的情形, 则有

$$\begin{aligned} & 2 + 4 + 6 + \cdots + 2k + 2(k+1) \\ &= (2 + 4 + 6 + \cdots + 2k) + 2(k+1) \\ &= k(k+1) + 2(k+1) \\ &= (k+1)(k+2) \end{aligned}$$

因此 $n=k+1$ 时 (3) 式也成立. 这样 (3) 式对一切自然数 n 都成立.

例 3 证明: n 边形的内角和等于 $(n-2)\pi$.

这是一个与多边形的边数 n 有关的命题. 由于多边形的边数至少是三个, 所以这个命题只与 3 以后的自然数有关, 即与 ≥ 3 的自然数有关. 这样用数学归纳法做证明时, 递推起点应该是 3. 一般地, 当一个命题 $P(n)$ 仅与 $\geq k_0$ 的自然数有关时, 用数学归纳法去做证明的递推起点就是 k_0 , 于是第一数学归纳法的格式为

1. 当 $n=k_0$ 时命题 $P(k_0)$ 成立;

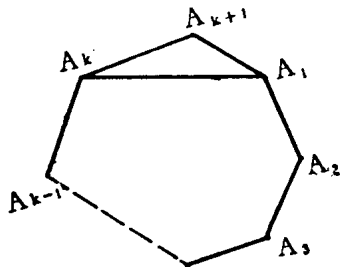
2. 假设当 $n=k \geq k_0$ 时命题 $P(k)$ 成立可推出 $n=k+1$ 时命题 $P(k+1)$ 也成立, 那么对一切 $\geq k_0$ 的自然数 n , 命题 $P(n)$ 都成立.

下面我们就用第一数学归纳法的这个格式来证明例 3. 此处 $k_0=3$. 事实上

1) 当 $n=3$ 时, 三角形的内角和等于 π , 即 $(3-2)\pi$, 所以命题 $P(3)$ 成立.

2) 假设当 $n=k \geq 3$ 时命题 $P(k)$ 成立, 看 $n=k+1$ 的情形.

这里需要推证的是 $k+1$ 边形的内角和等于 $(k-1)\pi$. 为此把以 $A_1, A_2, \dots, A_k, A_{k+1}$ 为顶点的 $k+1$ 边形 $[A_1A_2 \cdots A_kA_{k+1}]$ 分成两个多边形 (如右图): 一个是以



A_1, A_2, \dots, A_k 为顶点的 k 边形 $[A_1A_2 \cdots A_k]$, 另一个是以 A_1, A_k, A_{k+1} 为顶点的三角形 $[A_1A_kA_{k+1}]$. 于是

$$\begin{aligned} & [A_1A_2 \cdots A_kA_{k+1}] \text{的内角和} \\ &= [A_1A_2 \cdots A_k] \text{的内角和} + [A_1A_kA_{k+1}] \text{的内角和} \\ &= (k-2)\pi + \pi \\ &= (k-1)\pi, \end{aligned}$$

因此, 当 $n = k + 1$ 时命题 $P(k + 1)$ 也成立. 这样, 命题 $P(n)$ 对一切 ≥ 3 的自然数 n 都成立.

有些与自然数有关的命题 $P(n)$ 由于内容的内在特点, 命题 $P(k + 1)$ 不仅与命题 $P(k)$ 有联系, 而且与命题 $P(k), P(k - 1), \dots, P(2), P(1)$ 当中的某些个命题有联系. 这样, 单从命题 $P(k)$ 成立就推不出命题 $P(k + 1)$ 成立. 于是第一数学归纳法对这类命题的证明就用不上了. 为此我们有必要提出自然数集构成性质的另一表述形式, 即第二归纳原理, 从而相应的有第二数学归纳法.

第二归纳原理 设 M 是自然数集 N 的一个子集. 如果 M 具有以下两条性质:

1) 1 在 M 里;

2) 若 $\leq k$ 的自然数都在 M 里则 $k + 1$ 也在 M 里, 那么一切自然数都在 M 里, 即 $M = N$.

与第二归纳原理相应的有第二数学归纳法:

设 $P(n)$ 是与一切自然数有关的命题. 如果

1) 当 $n = 1$ 时命题 $P(1)$ 成立;

2) 假设对 $\leq k$ 的自然数 m 命题 $P(m)$ 都成立时可推出命题 $P(k + 1)$ 也成立, 那么命题 $P(n)$ 对一切自然数 n 都成立.

与第一数学归纳法一样, 第二数学归纳法的递推起点也可以是某一个大于 1 的自然数 k_0 .

例 4 设数列

$$a_1, a_2, a_3, \dots, a_n, \dots$$

其中 $a_1 = 3$, $a_2 = 7$, 而 $a_n = 3a_{n-1} - 2a_{n-2}$ ($n = 3, 4, \dots$).

试证通项公式为 $a_n = 2^{n+1} - 1$.

证 我们用第二数学归纳法来证明.

1) 当 $n = 1$ 时 $a_1 = 3$, $2^{1+1} - 1 = 3$, 所以对 $n = 1$ 公式成立;

2) 假设对 $n = 1, 2, \dots, k$ 时公式都成立, 看 $n = k + 1$ 的情形, 于是

$$a_{k+1} = 3a_k - 2a_{k-1} = 3(2^{k+1} - 1) - 2(2^k - 1) = 2^{k+2} - 1.$$

因此对 $n = k + 1$ 公式也成立. 这样对一切自然数 n , $a_n = 2^{n+1} - 1$ 都成立.

练习一

1. 证明 $1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

2. 证明 $1 \cdot 2 + 2 \cdot 3 + \dots + n(n+1) = \frac{n(n+1)(n+2)}{3}$.

3. 证明 $\frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \dots + \frac{1}{n(n+1)} = \frac{n}{n+1}$.

4. 证明 对一切自然数 n , $2^n > n$ 都成立.

5. 证明二项式公式:

$$(a+b)^n = a^n + c_1^n a^{n-1} b + \dots + c_r^n a^{n-r} b^r + \dots + b^n,$$

其中

$$c_r^n = \frac{n(n-1)\dots(n-r+1)}{r!}$$

是 n 个元素中取 r 个元素的组合数.

§ 2 整数的整除性

所谓整数就是 $\dots, -3, -2, -1, 0, 1, 2, 3, \dots$. 全体整数组成的数集记作 Z , 即

$$\mathbb{Z} : \dots, -3, -2, -1, 0, 1, 2, 3, \dots.$$

显然整数集 \mathbb{Z} 由三部分数合并而成，即

正整数 $1, 2, 3, \dots$;

负整数 $-1, -2, -3, \dots$;

数 0 ，这是唯一的不是正数也不是负数的整数。

整个这节都是复习性质的，一般叙述从简，论述较为详细之处则是必要的重复。

我们还是以运算为线索，从整数集 \mathbb{Z} 的运算性质谈起。

大家知道，整数集可以进行加法、减法和乘法运算。人们常把可以进行加、减、乘三种运算的数集叫做数环。整数集 \mathbb{Z} 构成的数环叫整数环。

在整数环里除法运算是不能进行的，因为并不是对任意两个整数 a 与 b ，其中 $b \neq 0$ ，都有唯一的整数 q 存在使

$$a = bq \tag{1}$$

成立。例如，尽管对 6 与 2 有整数 3 ，使

$$6 = 2 \cdot 3$$

成立，但没有哪一个整数 q ，能使

$$2 = 6 \cdot q$$

成立。当然对于 4 与 5 既没有使 $4 = 5 \cdot q$ 的整数 q 也没有使 $5 = 4 \cdot q$ 的整数 q 。于是虽然对某两个整数 a 与 b ($\neq 0$) 确有整数 q 使 (1) 式成立，但不是对每两个整数 a 与 b ($\neq 0$) 都有整数 q 使 (1) 式成立。所以整数集 \mathbb{Z} 不能进行除法。

这样，对于两个整数 a 与 b 是否有整数 q 使 (1) 式成立就成了整数集中两个整集 a 与 b 之间的一种特殊关系，由此引出了整除的概念。

设 $a, b \in \mathbb{Z}$ 。如果存在 $q \in \mathbb{Z}$ ，使

$$a = bq$$

成立，则称 (在 \mathbb{Z} 上) b 整除 a ，记作 $b \mid a$ ，否则就说 (在 \mathbb{Z} 上) b 不整除 a 。当 $b \mid a$ 时就说 b 是 a 的约数或说 b 是 a 的因数， a 是 b

的倍数。

整除是个基本概念，它有下列一些熟知的重要性质：

1) 若 $a \mid b$, $b \mid c$ 则 $a \mid c$, 这叫整除的传递性；

2) $a \mid b$ 又 $b \mid a$ 当且仅当 $b = \pm a$;

3) 若 $a \mid b$, $a \mid c$ 则 $a \mid (b \pm c)$;

4) 若 $a \mid b$ 或 $a \mid c$ 则 $a \mid bc$;

5) 设 a 为一确定的整数, x 为任意的整数。那么 $a \mid x$ 当且仅当 $a = \pm 1$; $x \mid a$ 当且仅当 $a = 0$ 。

这些性质都是容易验证的。我们只证明 2) 与 5) 这两条的正确性, 其它三条的证明做为练习留给读者。

事实上由 $a \mid b$ 又 $b \mid a$ 则有 $q_1, q_2 \in \mathbb{Z}$ 使

$$b = aq_1, a = bq_2$$

于是

$$b = bq_2q_1.$$

如果 $b = 0$ 那么显然也有 $a = 0$; 如果 $b \neq 0$ 那么可得 $q_2q_1 = 1$, 因为 q_1, q_2 都是整数, 从而必有 $q_1 = q_2 = 1$ 或 $q_1 = q_2 = -1$ 。这就得到 $b = \pm a$ 。反之, 如果 $b = \pm a$, 那么就有 $a = \pm b$ 。这就说明 $a \mid b$ 又 $b \mid a$, 性质 2) 被证明了。

再者, 如果 $a = \pm 1$, 那么对任一整数 x 显然都有 $a \mid x$ 。反之, 如果对任一整数 x 都有 $a \mid x$, 那么特别地取 $x = 1$, 当然也有 $a \mid 1$, 即 $1 = aq$, 从而必有 $a = \pm 1$ 。这样性质 5) 得到证明。

下面来说明公约数、最大公约数这两个概念。

如果 c 是 a 的约数也是 b 的约数, 则称 c 是 a 与 b 的公约数。

设 a, b 是不全为零的两个整数。于是在 a 与 b 的公约数中有绝对值为最大的, 称其为 a 与 b 的最大公约数, 简称为 a 与 b 的大公约。例如

4 与 6 的全体公约数是 1, -1, 2, -2, 于是 4 与 6 的大公约数为 2 和 -2; -4 与 -6 的全体公约数也是 1, -1, 2, -2, 因此 -4

与 -6 的大公约也是 2 和 -2 。再如 3 与 8 的全体公约数只有 $1, -1$ 这两个数, 这样 1 和 -1 就是 3 与 8 的大公约。

一般地, 如果 a 与 b 的大公约是 ± 1 , 就说 a 与 b 互质或互素。比如 3 与 8 互质、 4 与 9 也互质。

如上所见, a 与 b 的大公约是绝对值相同的两个数, 当中非负的那一个记作 (a, b) 。例如 $(4, 6) = 2, (-4, -6) = 2, (3, 8) = 1, (4, 9) = 1$ 。

如前所述, 由于整数集不能进行除法, 就使得在两个整数之间有了整除与不整除这种差别。现在我们把任二整数 a 与 b ($b \neq 0$) 用统一的形式联系起来, 使得整除关系是这种统一联系的一种特殊情形。这就是有名的

定理 1 (带余除法) 设 a, b 为任二整数, 但 $b \neq 0$ 。那么存在两个整数 q, r 使

$$a = bq + r \quad (2)$$

成立, 其中 $0 \leq r < |b|$ 。并且使(2)式成立的 q, r 只有一对。

例如 $a = 20, b = 3$ 时则有 $q = 6, r = 2$ 使 $20 = 3 \cdot 6 + 2; a = 20, b = -3$ 时则有 $q = -6, r = 2$ 使 $20 = (-3)(-6) + 2; a = -18, b = -3$ 时则有 $q = 6, r = 0$ 使 $-18 = (-3)6$ 。

下面给出定理 1 的证明。

由于 $a = bq + r$ 成立当且仅当 $a = (-b)(-q) + r$ 成立。因此我们可以仅就 b 是正整数的情形证明定理 1。我们考虑 b 的一切倍数:

$$\dots, -3b, -2b, -b, 0, b, 2b, 3b, \dots$$

于是只有两种可能, 即

1) a 恰好是 b 的某一个倍数, 即有 $q \in \mathbb{Z}$ 使 $a = bq$, 这就说明存在整数 $q, r = 0$ 使(2)式成立。

2) a 不是 b 的一个倍数, 因而 a 必在 b 的两个相邻倍数之间, 即有 $q \in \mathbb{Z}$ 使 $bq < a < b(q+1)$, 换个写法就有

$$a = bq + r, \text{ 其中 } 0 < r < b.$$

把以上两种可能的情形合起来写就有