

北京大学数学丛书

代 数 学

上 册

莫宗坚 蓝以中 赵春来 著



北 京 大 学 出 版 社

内 容 提 要

本书分上、下两册出版。

上册主要讲述近世代数的初步知识，内容包括集合论与数论、群论、多项式论、线性代数以及域论。

本书内容丰富，直观性强，推理自然，解释详尽。此书的独到之处是特别注重对于代数学的背景、基本思想以及与其它学科的联系等方面的介绍。书中精选了大量的例题和习题。本书的起点低，由浅入深。具有高等代数基础知识的读者就可以阅读本书，进而学到现代代数学的较大部分基础知识。

本书可作为高等学校数学系高年级学生以及研究生的教材，也可供数学工作者参考。

北京大学数学丛书

代 数 学

上 册

莫宗坚 等著

北京大学出版社出版

(北京大学校内)

北下关印刷厂印刷

新华书店北京发行所发行 各地新华书店经售

850×1168毫米 32开本 12印张 302千字

1986年10月第一版 1987年10月第二次印刷

印数：12001—17500册

统一书号：13209·140 定价：2.95元

上册目录

符号说明	(i)
第一章 集合论与数论	(1)
§ 1 集合论	(1)
§ 2 唯一分解定理	(7)
§ 3 同余式	(15)
§ 4 中国剩余定理	(22)
§ 5 复整数集	(26)
§ 6 p -adic 数与赋值	(37)
第二章 群论	(50)
§ 1 群的定义	(50)
§ 2 集合上的变换群	(57)
§ 3 子群	(63)
§ 4 内自同构及正规子群	(72)
§ 5 自同构群	(82)
§ 6 p 群及西洛定理	(87)
§ 7 若当-荷德定理	(93)
§ 8 对称群 S_n	(102)
第三章 多项式	(110)
§ 1 域与环	(110)
§ 2 多项式环及比域	(117)
§ 3 多项式环的唯一分解定理	(126)
§ 4 对称式, 结式及判别式	(141)
§ 5 理想	(157)

第四章 线性代数.....(175)

§ 1 向量空间.....(175)

§ 2 基及维数.....(180)

§ 3 线性变换及矩阵.....(191)

§ 4 模及主理想环上的模.....(206)

§ 5 若当标准式.....(226)

§ 6 内积及正交坐标.....(246)

§ 7 谱论.....(260)

第五章 一元多项式的解及域论.....(269)

§ 1 C 的代数封闭性.....(269)

§ 2 代数扩域.....(275)

§ 3 代数闭包.....(291)

§ 4 特征数及有限域.....(296)

§ 5 可离代数扩域.....(304)

§ 6 伽罗瓦理论.....(314)

§ 7 用根式解方程式.....(330)

§ 8 域多项式及判别式.....(343)

§ 9 超越扩张.....(349)

附 录 自然数的皮诺公理系.....(357)

汉英名词索引.....(362)

第一章 集合论与数论

§1 集合论

我们假定读者已熟悉集合论的基本概念，如交集、并集、子集、包含及映射等。请参考前面的“符号说明”。

定义1.1 设 S 及 T 为集合， $\rho: S \rightarrow T$ 是由 S 到 T 的映射。任取 S 中的二元素 s_1 及 s_2 ，如果 $\rho(s_1) = \rho(s_2)$ 时，必有 $s_1 = s_2$ ，则称 ρ 为一一映射，或单射。如果对于 T 中任意元素 t ，必有 $s \in S$ ，使 $\rho(s) = t$ ，则称 ρ 为 S 到 T 上的映射，或满射。如果 ρ 同时为单射及满射，则称 ρ 为单满映射。

集合论中最有意义的概念之一是“基数”。我们有如下的定义：

定义1.2 设 S 及 T 为集合。如有一单满映射 $\rho: S \rightarrow T$ ，则称 S 与 T 同基数。

讨论 1) 如集合 S 与整数集合 $\{1, 2, \dots, n\}$ 同基数，则称 S 为有限集，而称其基数为 n 。反之则称之为无限集。设 S 及 T 为同基数的有限集， $\rho: S \rightarrow T$ 为一映射，则易证：如 ρ 为单射，则 ρ 必为满射。反之，如 ρ 为满射，则 ρ 必为单射。此一命题可谓之鸽笼定理，即设想 S 为一群鸽子， T 为等数的鸽笼，则上命题即：如果每一鸽子已一一进笼，则鸽笼必无空者；反之，如鸽笼皆无空者，则必然每一笼中仅有一只鸽子。

2) 如集合 S 与正整数集合 $\{1, 2, 3, \dots, n, \dots\}$ 同基数，则称 S 为可数无限集。有限集与可数无限集统称可数集。除此之外，皆称为不可数集。

3) 对所有的无限集而言，鸽笼定理皆不成立，然而证法比较

复杂，远离本书的趣旨，请读者参考集合论的专书。现在我们仅举一例以说明此种现象，即所谓的“希尔伯特的旅馆”：设一旅馆有可数无限个房间 $\{1, 2, \dots, n, \dots\}$ ，已住满房客。如同时又来了可数无限个新房客 $\{g_1, g_2, \dots, g_n, \dots\}$ ，则一个简易的安排方法是令原住 n 号房间的老房客移入 $2n$ 号房间，于是空出 $\{1, 3, 5, \dots, 2n+1, \dots\}$ 所有奇数号房间。令新房客依序住入即可，也即令新房客 g_n 住入 $2n-1$ 号房间。从此例中，可以看出单射不一定必是满射。反之，如令头两个人挤一间房，其余的人依序住入空出的房间，则满射又不一定是单射了。

定理1.1 有理数集 $\mathbf{Q}$ 是可数无限集。

证明 我们采用所谓“三角数法”。考虑正有理数的集合 $\mathbf{Q}_+$ 。把 $\mathbf{Q}_+$ 中的元素按分母大小排成如下的无限矩阵：

$$\mathbf{Q}_+ = \begin{pmatrix} \frac{1}{1} & \frac{2}{1} & \frac{3}{1} & \dots \\ \frac{1}{2} & \frac{2}{2} & \frac{3}{2} & \dots \\ \frac{1}{3} & \frac{2}{3} & \frac{3}{3} & \dots \\ \dots & \dots & \dots & \dots \\ \frac{1}{n} & \frac{2}{n} & \frac{3}{n} & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix},$$

然后我们把整个矩阵的元素，按箭头所指的顺序，依次对应到所有正的偶数，自然，已经出现过的有理数则略去。例如，

$$\frac{1}{1} \rightarrow 2, \frac{1}{2} \rightarrow 4, \frac{2}{1} \rightarrow 6, \frac{1}{3} \rightarrow 8, \frac{3}{1} \rightarrow 10,$$

等等。这样就把 $\mathbf{Q}_+$ 对应到了正偶数集。同法，我们可以把负有理数集 $\mathbf{Q}_-$ 对应到大于1的正奇数集。再把0对应到1。不难看出，这个对应是由 $\mathbf{Q}$ 到正整数集 $\mathbf{N} = \{1, 2, \dots, n, \dots\}$ 的单满映射。

系 设有可数集 $S_i = \{s_{i1}, s_{i2}, \dots, s_{in}, \dots\}$, $i \in$ 可数集 I . 则这些可数个 S_i 的并集 $\bigcup_{i \in I} S_i$ 也是可数集.

定理1.2 实数集 $\mathbf{R}$ 为不可数集.

把 $r_1, r_2, \dots, r_n, \dots$ 用十进小数写出如下:

[illegible]

$$r = 0, c_1, c_2, \dots, c_n, \dots$$

在代数学中，经常应用构造“直积”、“商集”的方法。我们下定义。

定义1.3 设 I 为一个集合。如果对每一个 $i \in I$, 都有一个集合 S_i , 则 S_i 的直积 $\prod_{i \in I} S_i$ 定义为

$$\{(s_i)_{i \in I} : s_i \in S_i\},$$

即 I 到 $\bigcup_{i \in I} S_i$ 的所有映射 s , 而且能适合 $s(i) = s_i \in S_i$ 者. 如 I 为可数集时, $\prod_{i \in I} S_i$ 中的元素常写成一行 $(s_1, s_2, \dots, s_n, \dots)$.

3

即 $T = \bigcup_{i \in I} T_i$, 并且不同的子集 T_i 的交集为空集, 则这些子集 T_i

的集合 $\{T_i: i \in I\}$ 称为 T 的一个商集。

讨论 1) 设 T 为所有中国人民的集合, 按照某种法定年龄的标准, T 可以划分为 $T_1 =$ 未成年人的集合和 $T_2 =$ 成年人的集合。则 $\{T_1, T_2\}$ 构成 T 的一个商集。此商集中仅有两个元素。

2) 设 $\{T_i: i \in I\}$ 为 T 的一个商集, 则可在 T 中定义一个相应的“等价关系” $\sim$ 如下:

$$a \sim b \iff a, b \text{ 属于同一个 } T_i.$$

一般言之, 任意关系“ $\sim$ ”如具有下列三条性质, 则称为一个等价关系:

(a) 反身性: $a \sim a$;

(b) 对称性: 如果 $a \sim b$, 则 $b \sim a$;

(c) 传递性: 如果 $a \sim b$, $b \sim c$, 则 $a \sim c$ 。|

我们也可以用等价关系来定义商集如下。

定义 1.4* 设 $\sim$ 为集合 T 上的等价关系。令

$$T_a = \{b: b \in T, b \sim a\},$$

则 $\{T_a: a \in T\}$ 是 T 的一个商集, 称之为关于等价关系 $\sim$ 的商集, T_a 称为一个等价子集。

讨论 为说明定义 1.4* 中的 $\{T_a\}$ 确实是商集, 我们仅须验证两点: 1) $T = \bigcup_{a \in T} T_a$; 2) 如果 $T_a \cap T_c \neq \emptyset$, 则 $T_a = T_c$ 。1)

是显然的, 这因为 $a \sim a$, 所以 $a \in T_a$; 关于 2), 设 $b \in T_a \cap T_c$, 令 d 为 T_c 中任意元素, 则有

$$a \sim b \sim c \sim d, \quad a \sim c \sim d, \quad a \sim d.$$

即 $d \in T_a$ 。所以 $T_c \subset T_a$ 。同法可得出 $T_a \subset T_c$, 于是 $T_a = T_c$ 。|

下面的“数学归纳法”是正整数集 N 的公理之一, 其详情请见附录中正整数的“皮诺公理”。

数学归纳法 设对每个正整数 m , 有命题 $P(m)$ 。如能证明:

1) $P(1)$ 是正确的;

2) 设 n 是任意大于 1 的正整数。如对所有小于 n 的正整数 l , $P(l)$ 都是正确的, 则 $P(n)$ 是正确的,

那么所有的命题 $P(m)$ 皆是正确的。

讨论 这个数学归纳法不能从更简明的公理系统导出, 然而可以从下面的讨论中理解其合理性: 根据 1), 已知 $P(1)$ 是正确的。运用 2), 令 $n=2$, 则知 $P(2)$ 是正确的。再运用 2), 令 $n=3$, 则知 $P(3)$ 是正确的。如此反复运用 2), 则知所有的命题 $P(m)$ 皆是正确的。|

在代数学里, 经常应用“Zorn引理”。此引理等同于“选择公理”及“良序原理”, 是集合论的公理之一。为了讨论Zorn引理, 我们先引入“序”与“半序”的概念。

定义1.5 设 S 为一集合。 S 的一个关系“ $\geq$ ”如适合下列条件, 则称之为一个半序:

1) $s_1 \geq s_1, \forall s_1 \in S$;

2) $s_1 \geq s_2, s_2 \geq s_3 \implies s_1 \geq s_3, \forall s_1, s_2, s_3 \in S$;

3) $s_1 \geq s_2, s_2 \geq s_1 \implies s_1 = s_2, \forall s_1, s_2 \in S$ 。

定义1.6 设 S 为一集合, $\geq$ 为 S 的半序。如果适合下列条件, 则称 $\geq$ 为 S 的序:

4) 对任意的 $s_1, s_2 \in S$, 总有 $s_1 \geq s_2$ 或 $s_2 \geq s_1$ 。

定义1.7 设 $\geq$ 为 S 的半序, T 为 S 的子集。如果 S 的一个元素 s , 适合 $s \geq t (\forall t \in T)$, 则称 s 为 T 的一个上限。如果 s 具有如下性质: $\forall s_1 \in S$, 只要 $s_1 \geq s$, 必有 $s_1 = s$, 则称 s 为 S 的一个极大元素。

定义1.8 设 S 为一集合, $\geq$ 为 S 的半序, T 为 S 的子集。如果局限于 T 中 $\geq$ 是一个序, 则称 T 为一链。

Zorn引理 设 S 为一非空集合, $\geq$ 为 S 的半序。如果任意链皆有上限, 则 S 有一极大元素。

讨论 1) 在集合论中, 已经证明了 Zorn 引理实际上是一个

公理，所以不可能从其它较简单的公理系统中导出。

2) 利用 Zorn 引理可以简化许多证明，也可以证明一些除此之外的其它方法不能证明的结果。例如，我们可以证明平面上的任何有界区域 D 内皆有极大的开圆盘，证法如下：(a) 令 S 为 D 内所有开圆盘构成的集合，用包含 $\subset$ 定义半序 $\leq$ ；(b) 由于 D 内至少有一个开圆盘，所以 S 是非空的；(c) 如果一些开圆盘构成的集合 $\{D_i: i \in I\}$ 成为一链，则 $\bigcup_{i \in I} D_i$ 也显然是 D 的一个开圆盘，它是此链的上限；(d) 于是根据 Zorn 引理，有界区域 D 内必有极大的开圆盘。

习 题

1. 设 ρ 为集合 S 到集合 T 的映射。证明 ρ 是一个单射的充要条件是下列两条件中任一条成立：

(1) 存在 T 到 S 的映射 τ ，使 $\tau\rho = 1_S$ ；

(2) 不存在某集合 U 到 S 的两个不同映射 τ_1, τ_2 ，使

$$\rho\tau_1 = \rho\tau_2.$$

2. 设 ρ 为集合 S 到集合 T 的映射。证明 ρ 是一个满射的充要条件是下列两条件中任一条成立：

(1) 存在 T 到 S 的映射 τ ，使 $\rho\tau = 1_T$ ；

(2) 不存在 T 到某集合 U 的两个不同映射 τ_1, τ_2 ，使

$$\tau_1\rho = \tau_2\rho.$$

3. 设 S 是一基数为 $n(n \geq 1)$ 的有序集。证明在 S 中存在一个元素 a ，使 $\forall b \in S$ ，有 $a \leq b$ 。举例说明无限的有序集不一定具有此性质。

4. 设 ρ 是集合 S 到集合 T 的映射， A, B 是 S 的子集。证明 $\rho(A \cup B) = \rho(A) \cup \rho(B)$ ， $\rho(A \cap B) \subset \rho(A) \cap \rho(B)$ 。

举例说明 $\rho(A \cap B)$ 不一定等于 $\rho(A) \cap \rho(B)$ 。

5. 设 ρ 是集合 S 到集合 T 的映射， A 是 S 的子集。证明在

一般情况下 $\rho(S \setminus A) \not\subset T \setminus \rho(A)$.

6. 设 $\omega_1, \omega_2 \in \mathbf{C}$, 且 $\omega_1/\omega_2 \in \mathbf{R}$. 在 $\mathbf{C}$ 内定义等价关系:

$$a \sim \beta \iff \beta = a + a\omega_1 + b\omega_2 \quad (a, b \in \mathbf{Z}).$$

试求 $\mathbf{C}$ 对上述等价关系的商集.

7. 令 $\mathbf{Q}[x]$ 表示所有有理系数的多项式集. 证明 $\mathbf{Q}[x]$ 是一个可数集.

8. 令 C 表 Cantor 点集. C 的构造法如次: 在区间 $[0, 1]$ 中挖去中间的 $1/3$ 长的开线段 $(1/3, 2/3)$. 其次, 在所余的两个闭线段 $[0, 1/3]$, $[2/3, 1]$ 中各挖去中间的 $1/3$ 长的开线段. 如此反复作下去, 所得的余集即是 C . 证明 C 是一个不可数集.

9. 证明“兄弟”是一个等价关系, “子女”不是一个等价关系.

10. 证明在整数集 $\mathbf{Z}$ 中, 通常用的“ $\geq$ ”是一个序.

11. 证明在任何一个集合 S 中, 包含“ $\supset$ ”是子集族的一个半序.

12. 证明题10中的半序不适合 Zorn 引理的条件, 而题11中的半序适合之.

§ 2 唯一分解定理

数学的起源之一是对整数的研究. 近世代数从整数的“皮诺公理系”开始讨论, 由此公理系引出整数集的四则运算的法则, 如交换律、结合律、分配律等, 并进一步建构有理数集 $\mathbf{Q}$ 、实数集 $\mathbf{R}$ 、复数集 $\mathbf{C}$. 这种讨论法自有其逻辑的严谨性, 然而对于代数学的读者而言, 似嫌迂远, 旁离本旨. 本书将这部分的推理列入附录中. 以下我们将假设读者已熟悉整数集 $\mathbf{Z}$ 、有理数集 $\mathbf{Q}$ 、实数集 $\mathbf{R}$ 及复数集 $\mathbf{C}$ 的四则运算的法则.

整数论中, 最重要的定理之一是“辗转相除法”. 汉代的数学书《九章算术》中, 有求两正整数的公因数的“更相减损求

等”之法，即“辗转相除法”也。秦九韶于《数书九章》（1247年）又曾论及。在现代，此法通常被称为“欧几里得算法”。我们先引入如下的概念。

定义1.9 设 a 为一实数，以 $[a]$ 表示小于或等于 a 的最大整数，即 a 的整数部分。

讨论 例如， $[3.1] = 3$ ， $[-3.1] = -4$ ， $[5] = 5$ 。

定理1.3(欧几里得算法) 令 d 为一正实数， n 为任意实数。则必有一整数 q 及一实数 r ，使得

$$n = qd + r, \quad 0 \leq r < d.$$

证明 应用定义1.9，读者自证。|

系1 在以上定理中， q 及 r 皆为唯一确定的。

证明 读者自证。|

系2 如在上定理中 n 及 d 皆为整数，则 r 也为整数。

欧几里得算法的应用之一是研究几个整数的因数及公因数。为此，我们定义如下：

定义1.10 设 a, b, c 为整数。如果 $a = bc$ ，则称 a 是 b 的倍数， b 是 a 的因数，用符号 $b|a$ 表示之。如果 $b|a_1, b|a_2, \dots, b|a_n$ ，则称 b 是 $a_1, a_2, \dots, a_n$ 的公因数。 $a_1, a_2, \dots, a_n$ 的公因数中的最大者，称为 $a_1, a_2, \dots, a_n$ 的最大公因数。如果 $b_1|a, b_2|a, \dots, b_m|a$ ，则称 a 是 $b_1, b_2, \dots, b_m$ 的公倍数。 $b_1, b_2, \dots, b_m$ 的公倍数中最小非负整数，称为 $b_1, b_2, \dots, b_m$ 的最小公倍数。如果 a 与 b 的最大公因数是1，则称 a 与 b 互素。

定理1.4 设 $a_1, a_2 \in \mathbf{Z}$ ，且 a_1, a_2 不全为零，则 a_1, a_2 的最大公因数是集合

$$(a_1, a_2) = \{b_1 a_1 + b_2 a_2 : b_1, b_2 \in \mathbf{Z}\}$$

中的最小正整数。

证明 令集合 (a_1, a_2) 中的最小正整数为

$$d = c_1 a_1 + c_2 a_2, \quad c_1, c_2 \in \mathbf{Z}.$$

按照欧几里得算法, 存在整数 q_1 及 r_1 , 使得

$$a_1 = q_1 d + r_1, \quad 0 \leq r_1 < d.$$

如果 $r_1 \neq 0$, 则有

$$r_1 = a_1 - q_1 d = (1 - c_1 q_1) a_1 + (-q_1 c_2) a_2 \in (a_1, a_2),$$

即 r_1 是 (a_1, a_2) 中比 d 更小的正整数. 这显然是不可能的. 故知 $r_1 = 0$, 即

$$a_1 = q_1 d,$$

亦即

$$d | a_1.$$

同法可证 $d | a_2$. 即 d 是 a_1, a_2 的公因数.

现设 d' 为 a_1, a_2 的另一公因数, 则有

$$d' | a_1, d' | a_2 \implies d' | c_1 a_1 + c_2 a_2,$$

即 $d' | d$. 而 d 为正整数, 故 $d \geq d'$. |

以下, 我们将证明“算术基本定理”. 即整数分解成“素数”的连乘积的“唯一分解定理”. 为此, 我们要引入“不可约数”及“素数”的概念. 值得注意的是, 在整数集中有乘法逆元素的数仅是 1 与 -1 , 即如果 n 与 n^{-1} 皆为整数, 则 n 必为 1 或 -1 .

定义 1.11 设有一整数 a , 非 $0, 1, -1$. 如在 a 的任意分解式 $bc = a$ 中, 必有 b 或 c 为 1 或 -1 (即 b 和 c 之一必为可逆的), 则称 a 是一个不可分解数 (或称不可约数). 如果 $a | fg$ 时, 必有 $a | f$ 或 $a | g$, 则称 a 是一个素数. 素数又称为质数.

引理 $\mathbb{Z}$ 的不可约数皆是素数, 素数也皆是不可约数,

证明 设 a 是不可约数, 不妨设 $a > 0$ (否则讨论 $-a$). 设 $a | bc$. 如果 a 不是 b 的因数, 由于 a 的正因数只有 1 与 a , 所以 a, b 的最大公因数必为 1. 按照定理 1.4, 有 $c_1, c_2 \in \mathbb{Z}$, 使得

$$1 = c_1 a + c_2 b.$$

以 c 乘上式两边, 得到

$$c = c(c_1a + c_2b) = \left(cc_1 + c_2 \left(\frac{bc}{a} \right) \right) a.$$

由于 $a|bc$, 故 $bc/a \in \mathbf{Z}$. 由上式即知 $a|c$. 所以 a 为素数. 反之, 设 a 为素数, 且 $a = bc$. 不妨设 $a|b$, 则 a, b 的最大公因数必为 $|a|$ 及 $|b|$, 于是有 $|a| = |b|$, 故 $c = \pm 1$. $\square$

讨论 从上面的引理可以看出, 在 $\mathbf{Z}$ 中“不可约数”与“素数”是一物的二名. 在以后的“环论”中可以看到, 在广泛的情况下, 这两个概念是各有所指的. 这两个概念的同一性是下面的“唯一分解定理”的基石.

定理 1.5 (唯一分解定理) 任意大于 1 的整数 a 皆可分解成正素数的连乘积

$$a = \prod_i p_i.$$

在这个连乘积中, 正素数 p_i 的次序自然可以调换. 除此之外, 这个连乘积是唯一的.

证明 我们首先证明这个分解是存在的, 然后再证明其唯一性.

2 是正素数, 于是 $2 = 2$ 是 2 的分解. 按照数学归纳法, 给定一个正整数 $a > 1$, 可以假定所有大于 1 小于 a 的整数皆可分解. 如果 a 是素数, 则 $a = a$ 是 a 的分解; 如果 a 不是素数, 应用引理, 得到

$$a = bc, \quad a > b > 1, \quad a > c > 1,$$

其中 b 及 c 皆可分解成正素数连乘积, 于是 a 可分解为正素数连乘积, 即 $a = \prod_i p_i$.

下面证分解的唯一性. 设 $a = \prod_i q_i$ 是 a 的另一正素数连乘积分解式, 则有

$$p_1 | a = q_1 \left(\prod_{i>1} q_i \right),$$

于是有

$$p_1 | q_1 \quad \text{或} \quad p_1 \left| \left(\prod_{j>1} q_j \right) \right|.$$

如果 $p_1 \nmid q_1$, 则必有 $p_1 \left| q_2 \left(\prod_{j>2} q_j \right) \right|$, 于是有

$$p_1 | q_2 \quad \text{或} \quad p_1 \left| \left(\prod_{j>2} q_j \right) \right|.$$

如此推演下去, 必有某个 q_s , 使得

$$p_1 | q_s.$$

而 q_s 为素数, 由引理, q_s 为不可约数, 于是有

$$q_s = p_1.$$

考虑

$$\prod_{i>1} p_i = \frac{a}{p_1} = \frac{a}{q_s} = \prod_{j>1} q_j,$$

应用数学归纳法, 即有唯一性。I

以后, 除特别声明外, 所谓“素数”皆指正素数而言。

例1 不难导出下述命题: “设 p_i ($i=1, 2, \dots, n$) 均为素数,

则 $\left(\prod_{i=1}^n p_i \right) + 1$ 的因数皆非 $p_1, p_2, \dots, p_n$ 。”这是因为, 如果 p_j 为

$\left(\prod_{i=1}^n p_i \right) + 1$ 的因数, 则有 $a \in \mathbf{Z}$, 使得

$$ap_j = \left(\prod_{i=1}^n p_i \right) + 1,$$

即

$$\left(a - \prod_{i \neq j} p_i \right) p_j = 1,$$

也即 $p_j | 1$ 。这显然是不可能的。由上面这个命题, 又可推出“素数有无限多个”。事实上, 如果仅有有限多个素数 $p_1, p_2, \dots, p_n$,

则 $(\prod_{i=1}^n p_i) + 1$ 的素因子只能是 $p_1, p_2, \dots, p_n$ 中的某些个, 这与上面的命题矛盾。故知素数有无限多个。

例 2 取一正分数 m/n , 可以用欧几里得算法求得其连分数。我们且举祖冲之(430—501年)的“密率” $\frac{355}{113}$ 为例。

$$\begin{aligned}\frac{355}{113} &= \frac{3 \times 113 + 16}{113} = 3 + \frac{16}{113} = 3 + \frac{1}{\frac{113}{16}} \\ &= 3 + \frac{1}{\frac{7 \times 16 + 1}{16}} = 3 + \frac{1}{7 + \frac{1}{16}}.\end{aligned}$$

更一般地, 任意实数 r , 都可以用此法求出其连分数。我们以 $\pi = 3.14159265358979323846\dots$ 为例, 以说明之。

$$\begin{aligned}\pi &= \frac{\pi}{1} = 3 + \frac{0.14159265358979323846\dots}{1} \\ &= 3 + \frac{1}{\frac{1}{0.14159265358979323846\dots}} \\ &= 3 + \frac{1}{7 + \frac{0.00885142787144737077\dots}{0.14159265358979323846\dots}} \\ &= 3 + \frac{1}{7 + \frac{1}{\frac{0.14159265358979323846\dots}{0.00885142787144737077\dots}}} \\ &= 3 + \frac{1}{7 + \frac{1}{15 + \frac{0.00882123551809317691\dots}{0.00885142787144737007\dots}}}\end{aligned}$$

$$= 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1 + \frac{0.00885142787144737007\cdots}{0.00003019235335419316\cdots}}}}$$

$$= 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1 + \frac{1}{292 + \cdots}}}}.$$

这种连分数与“最佳渐近分数”有关，详见华罗庚著《数论导引》第十章。在上面的 π 的连分数中，如果我们只保留前边几项，弃去其余的项，则得到

$$3, \quad 3 + \frac{1}{7}, \quad 3 + \frac{1}{7 + \frac{1}{15}}, \quad 3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1}}},$$

$$3 + \frac{1}{7 + \frac{1}{15 + \frac{1}{1 + \frac{1}{292}}}},$$

也即

$$3, \quad \frac{22}{7}, \quad \frac{333}{106}, \quad \frac{355}{113}, \quad \frac{103993}{33102},$$

而祖冲之的“密率”适在其中。

习 题

1. 设 n 为正整数， a 为实数。证明：

$$(1) \quad \left[\frac{[na]}{n} \right] = [a],$$