SERIES ON UNIVERSITY MATHEMATICS VOL. 5

# ALGEBRA

T T Moh

代数学

2

World Scientific

世界图书出版公司
www.wpcbj.com.cn

SERIES ON UNIVERSITY MATHEMATICS VOL. 5

# ALGEBRA

T T Moh
Department of Mathematics
Purdue University
USA

World Scientific
Singapore • New Jersey • London • Hong Kong

*Published by*

World Scientific Publishing Co. Pte. Ltd.
P O Box 128, Farrer Road, Singapore 9128
*USA office:* Suite 1B, 1060 Main Street, River Edge, NJ 07661
*UK office:* 57 Shelton Street, Covent Garden, London WC2H 9HE

First published 1992
First reprint 1995

**ALGEBRA**

ISBN 981-02-1195-3
ISBN 981-02-1196-1 (pbk)

图书在版编目（CIP）数据

代数学＝Algebra：英文／（美）莫（Moh，T．T．）著．—北京：世界图书出版公司北京公司，2008.12
ISBN 978-7-5062-9263-4

Ⅰ.代… Ⅱ.莫… Ⅲ.代数-研究生-教材-英文
Ⅳ.015

中国版本图书馆CIP数据核字（2008）第195296号

| | | | |
|---|---|---|---|
| 书　　名： | Algebra | | |
| 作　　者： | T T Moh | | |
| 中 译 名： | 代数学 | | |
| 责任编辑： | 高蓉 刘慧 | | |
| 出 版 者： | 世界图书出版公司北京公司 | | |
| 印 刷 者： | 三河国英印务有限公司 | | |
| 发　　行： | 世界图书出版公司北京公司（北京朝内大街 137 号　100010） | | |
| 联系电话： | 010-64015659 | | |
| 电子信箱： | kjsk@vip.sina.com | | |
| 开　　本： | 16开 | | |
| 印　　张： | 23 | | |
| 版　　次： | 2009 年 01月第 1 次印刷 | | |
| 版权登记： | 图字:01-2008-5578 | | |
| 书　　号： | 978-7-5062-9263-4/ O • 648 | 定　　价: | 55.00 元 |

# PREFACE

*Algebra is generous : she often gives more than is asked of her.*

D'Alembert

The present book comes from the first part of the lecture notes I used for a first-year graduate algebra course at the University of Minnesota, Purdue University, and Peking University. The Chinese versions of these notes were published by The Peking University Press in 1986, and by Linking Publishing Co of Taiwan in 1987.

The aim of this book is not only to give the student quick access to the basic knowledge of algebra, either for future advancement in the field of algebra, or for general background information, but also to show that algebra is truly a master key or a 'skeleton key' to many mathematical problems. As one knows, the teeth of an ordinary key prevent it from opening all but one door, whereas the skeleton key keeps only the essential parts, allowing it to unlock many doors.

Sometimes I like to think that 'fashion' is a space-traveler, while 'wisdom' is a time-traveler. Frequently, the time-traveler only touches a small circle among the elite. Most people think that Mathematics is dry and difficult. Most mathematicians feel the same way towards algebra. How unfortunate! When Heisenberg presented his quantum theory, he had to re-invent matrix theory. Mathematicians, and algebraists especially, should present the subject more interestingly to attract the attention of the student and the concerned reader.

I wish to present this book as an attempt to help the student to re-establish the contacts between algebra and other branches of mathematics and sciences. I prefer the intuitive approaches to algebra, and have included many examples and exercises to illustrate its power. I hope that the present book fulfills these goals.

To teach a core course for one semester, the materials of §6, Chapter I, §7, Chapter II, §4, Chapter III, §3 -§7, Chapter IV, part of §3 and §8 -§9, Chapter V may be omitted.

We wish to thank Jem Corcoran for proof-reading.

*T.T.Moh*
*W. Lafayette, 1992*

## CONTENTS

# CHAPTER I

# Set Theory and Number Theory

## §1 Set Theory

We shall assume the elementary concepts of set[1] theory in this book as the *union*, the *intersection*, the *inclusion* and the *mapping*. The set theory symbols used in this book will be listed in the appendix I.

**Definition 1.1.** *Let* S *and* T *be sets,* $\rho$: S $\to$ T *be a map from the set* S *to the set* T. *If* $\rho(s_1) = \rho(s_2)$ *implies* $s_1 = s_2$ *for any two elements* $s_1, s_2 \in$ S, *then we say the map* $\rho$ *is 1–1 or injective. If for any given* $t \in$ T, *there is a* $s \in$ S *with* $\rho(s) = t$, *then we say the map* $\rho$ *is onto or surjective. If* $\rho$ *is injective and surjective, then we say that* $\rho$ *is bijective.* ▮

One of the most important concepts in the set theory is the *cardinal number*. We have the following definition,

**Definition 1.2.** *Let* S *and* T *be sets. If there is a bijective map* $\rho$: S $\to$ T, *then we say that* S *and* T *have the same cardinality.* ▮

**Discussion**

(1) If the cardinalities of the set S and the set of integers $\{1, 2, \cdots, n\}$ are the same, then we say the set S is a *finite set*, and the cardinality of S is $n$. Otherwise, the set S is said to be an *infinite set*. Furthermore, if the cardinalities of the set S and the set of all positive integers $\{1, 2, \cdots, n, \cdots\}$ are the same, then we say that the set S is a *countably infinite set*. If a set S is either finite or countably infinite, then we say the set S is *countable*. If the set S is not countable, then we say the set S is *uncountable*.

[1] Due to German Mathematician Cantor 1874.

Certainly the set of non-negative integers $\{0, 1, 2, 3, 4, \cdots\}$ is countable. Furthermore the set of all integers $\mathbf{Z}$ can be listed as $\{0, -1, 1, -2, 2, \cdots, -i, i, \cdots\}$, hence is also countable.

(2) ***Pigeon hole principle***: Given two finite sets **S** and **T** with the same cardinality. Let $\rho$ be a map $\mathbf{S} \to \mathbf{T}$. Then $\rho$ is injective $\Leftrightarrow$ surjective $\Leftrightarrow$ bijective.

One may imagine that the set **S** is a finite set of pigeons and the set **T** is the set of the pigeon holes with the same cardinality. Then the above principle says that if every pigeon gets into a different hole, then every hole is occupied. On the other hand, if every hole is occupied, then every pigeon must get into a different hole.

(3) In fact, the pigeon hole principle is true only for the finite cardinalities. If a set **S** is infinite, then it follows from the set theory (using some form of the ***axiom of choice***) that there is a countably infinite subset **R**. It is easy to use the argument of ***Hilbert's hotel*** as follows to show that the pigeon hole principle is false: let there be a hotel with countably infinite many rooms $\{r_1, r_2, \cdots\}$ filled with guests $\{g_1, g_2, \cdots\}$. Suppose that there appear countably infinite many new guests $\{n_1, n_2, \cdots\}$. A simple way of management is to ask the old guest $g_m$ to move to the room $r_{2m}$, and assign the new guest $n_m$ to the room $r_{2m-1}$. It is clear that all guests, old or new, will each have a room. Imitating this example, the reader will have no trouble to set a mapping $\rho$: $\mathbf{R} \to \mathbf{R}$ which is injective while not surjective. Furthermore, we may extend the map $\rho$ to **S** by defining $\rho(s) = s$ for all $s \notin \mathbf{R}$. Then it is easy to see the extension of $\rho$ is injective while not surjective. On the other hand, we may require the first two guests $g_1, g_2$ to stay in the first room $r_1$, while the guest $g_m$ stays in the room $r_{m-1}$ for all $m \geq 3$. Then we construct a map which is surjective while not injective. ∎

**Theorem 1.1.** *Let the sets* $\mathbf{S}_i$ *be countable sets for* $i = 1, 2, \cdots$. *Then the union set* $\mathbf{S} = \bigcup_{i=1}^{\infty} \mathbf{S}_i$ *is a countable set.*

*Proof*: Let the set $\mathbf{S}_i = \{a_{i1}, a_{i2}, \cdots, a_{ij}, \cdots\}$. We shall use the following *triangle counting* to form a sequence,

$$\begin{array}{l}
a_{11}, a_{12}, a_{13}, \cdots, a_{1j}, \cdots \\
\quad \nearrow \quad \nearrow \quad \nearrow \qquad\quad \nearrow \\
a_{21}, a_{22}, a_{23}, \cdots, a_{2j}, \cdots \\
\quad\quad \nearrow \quad \nearrow \qquad\qquad \nearrow \\
a_{31}, a_{32}, a_{33}, \cdots, a_{3j}, \cdots \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots \\
\quad \nearrow \quad \nearrow \quad \nearrow \qquad\quad \nearrow \\
a_{i1}, a_{i2}, a_{i3}, \cdots, a_{ij}, \cdots \\
\cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots
\end{array}$$

In other words, let us define a sequence $\{c_1, c_2, \cdots, c_k, \cdots\}$ with $c_k = a_{ij}$ where $k = ((i + j - 1)(i + j - 2)/2) + j$. In this sequence let us delete all $c_k$ which equals to $c_n$ for some $n < k$. Then it is obvious that the set of the deleted sequence is the union set **S**. Thus we establish that the union set **S** is countable. ∎

**Corollary.** *The set of rational numbers* $\mathbf{Q}$ *is countable.*

*Proof*: We always have $\mathbf{Q}=\bigcup_{i=1}^{\infty}\frac{1}{i}\mathbf{Z}$, while $\frac{1}{i}\mathbf{Z}$ is a countable set for each $i$. Our Corollary follows from the preceding Proposition. ■

**Theorem 1.2.** *The set of real numbers* $\mathbf{R}$ *is uncountable.*

*Proof*: Suppose that the set of real numbers $\mathbf{R}$ is countable, i.e., $\mathbf{R}=\{r_1, r_2, \cdots, r_i, \cdots\}$. We will use the following ***diagonal counting*** to deduce a contradiction.

Let $r_i$ be expressed as the decimal number $r_i = a_i.b_{i1}b_{i2}\cdots b_{ij}\cdots$, where $a_i$ is the integer part of $r_i$ and $0 \le b_{ij} \le 9$. We have the following diagram,

$$\begin{array}{c}
r_1{=}a_1.b_{11}b_{12}\cdots b_{1j}\cdots\\
r_2{=}a_2.b_{21}b_{22}\cdots b_{2j}\cdots\\
r_3{=}a_3.b_{31}b_{32}\cdots b_{3j}\cdots\\
\cdots\cdots\cdots\cdots\cdots\cdots\\
\cdots\cdots\cdots\cdots\cdots\cdots\\
r_i{=}a_i.b_{i1}\,b_{i2}\cdots b_{ij}\cdots\\
\cdots\cdots\cdots\cdots\cdots\cdots
\end{array}$$

Although there are some ambiguities about the decimal expressions of the real numbers, i.e., $2.340000\cdots = 2.339999\cdots$, however, it will not interfere with the following arguments. Let the real number $r = 0.c_1c_2\cdots c_i\cdots$ be defined $c_i = 5$ if $b_{ii} \neq 5$, otherwise $c_i = 4$. Then $r$ is a real number which is not in the list $\{r_1, r_2, \cdots, r_i, \cdots\}$. Thus we establish that the set of real numbers $\mathbf{R}$ is not countable. ■

In Algebra the processes of taking the "***direct product***" and "***quotient***" are commonly used. Their definitions are given as follows,

**Definition 1.3.** *Let* $\{\mathbf{S}_i\}$, $i \in \mathbf{I}$, *be a collection of sets* $\mathbf{S}_i$. *Then the direct product of the set* $\{\mathbf{S}_i\}$, $\prod_{i\in I}\mathbf{S}_i$, *is defined to be the set* $\{(s_i)_{i\in I} : s_i \in \mathbf{S}_i\}$, *i.e., the set of all maps* $s : I \to \bigcup_{i\in I}\mathbf{S}_i$ *with* $s(i) = s_i \in \mathbf{S}_i$. *The set* $\mathbf{I}$ *will be called as the **index set** of the direct product. If the index set* $\mathbf{I}$ *is the set of positive integers* $\mathbf{Z}_+$, *sometimes we write the elements of the direct product as the sequences* $\{s_1, s_2, \cdots\}$. ■

**Definition 1.4.** *Let* $\mathbf{T}$ *and* $\mathbf{I}$ *be sets, and let* $\mathbf{T}_i$, $i \in\mathbf{I}$, *be subsets of* $\mathbf{T}$ *such that* $\mathbf{T}$ *is a **disjoint union** of* $\mathbf{T}_i$, *i.e.,* $\mathbf{T}=\bigcup_{i\in I}\mathbf{T}_i$ *and* $\mathbf{T}_i\bigcap\mathbf{T}_j = \emptyset$ *for* $i \neq j$, *then the set of the subsets* $\{\mathbf{T}_i\}$ *is called a **quotient set** of* $\mathbf{T}$. ■

**Discussion**

(1) Let $\mathbf{T}$ be the set of the people of a country. According to the law, the set $\mathbf{T}$ may be separated into the subsets: $\mathbf{T}_1$ = the set of all juveniles and $\mathbf{T}_2$ = the set of all adults. Then $\{\mathbf{T}_1, \mathbf{T}_2\}$ is a quotient set of $\mathbf{T}$ with two elements.

(2) Another way to discuss the quotient set is through the concept of ***equivalence relations*** which is defined as follows. A relation "$\sim$" is said to be an equivalence relation if and only if the following conditions are satisfied,

(r) Reflexion: $t \sim t$ for all $t \in \mathbf{T}$.

(s) Symmetry: $t \sim s \Longrightarrow s \sim t$.

(t) Transition: $t \sim s, s \sim r \Longrightarrow t \sim r$.

(3) Let $\{\mathbf{T}_i\}$ be a quotient set of $\mathbf{T}$. Then we may define a relation "$\approx$" as follows,

$$t \approx s \Longleftrightarrow t, s \in \text{ the same } \mathbf{T}_j$$

Then it is easy to see that the relation $\approx$ is indeed an equivalence relation.

(4) Suppose that we are given an equivalence relation $\sim$. Let the subset $\mathbf{T}_t$ be defined as $\mathbf{T}_t = \{s : s \sim t\}$. Then it is easy to see that $\mathbf{T}$ is a disjoint union of $\{\mathbf{T}_t\}$. Hence $\{\mathbf{T}_t\}$ is a quotient set of $\mathbf{T}$. ∎

To sum up the above discussions (3) & (4), we have the following new definition,

**Definition 1.4*.** *Let "$\sim$" be an equivalence relation on a set* $\mathbf{T}$. *Let* $\mathbf{T}_t = \{s : s \sim t\}$. *The subset* $\mathbf{T}_t$ *is called an equivalence subset of* $\mathbf{T}$. *Then* $\{\mathbf{T}_t\}$ *is a called the quotient set of* $\mathbf{T}$ *with respect to the relation "$\sim$".* ∎

Let us now introduce one of the axioms, *Mathematical induction*, for the set of positive integers $\mathbf{Z}_+$ as follows, for a detailed discussion, the reader is referred to Appendix II.

**Mathematical induction:** Let $\{\mathrm{P}(i)\}_{i \in Z_+}$ be a set of statements indexed by the set of positive integers $\mathbf{Z}_+$. If we can verify that

(a) the statement $\mathrm{P}(1)$ is true.

(b) for $n \geq 2$, the truth of $\mathrm{P}(\ell)$ for all $\ell < n$ implies the truth of $\mathrm{P}(n)$.

then $\mathrm{P}(n)$ is true for all positive integers $n$. ∎

**Discussion**

(1) Mathematical induction is an axiom satisfied by the set of positive integers $\mathbf{Z}_+$. Although it can not be deduced from a small set of axioms, we may understand the rationale of it; it follows from (1) above, we know that $\mathrm{P}(1)$ is true. Furthermore, let $n = 2$ in (2), we may conclude that $\mathrm{P}(2)$ is true. Then let $n = 3$ in (2), we conclude that $\mathrm{P}(3)$ is true. Recursively, we conclude that $\mathrm{P}(n)$ is true for all $n$. ∎

We shall use *Zorn's lemma* very often in Algebra. It is known that Zorn's lemma is equivalence to the *axiom of choice* and the *well ordering principle.* Although it is an axiom of the set theory which can not be proved, it is important to understand Zorn's lemma. For this purpose, let us introduce the concepts of the *partial ordering* and the *total ordering.* Sometime a total ordering is simply called an *ordering.*

**Definition 1.5.** *Given a set* $\mathbf{T}$ *and a relation* $\geq$ *on* $\mathbf{T}$. *If the relation* $\geq$ *satisfies the following conditions, then it is called a partial ordering,*

(a) $t_1 \geq t_1$ *for all* $t_1 \in \mathbf{T}$.

(b) $t_1 \geq t_2$ *and* $t_2 \geq t_3 \Longrightarrow t_1 \geq t_3$.

(c) $t_1 \geq t_2$ *and* $t_2 \geq t_1 \Longrightarrow t_1 = t_2$. ∎

**Definition 1.6.** *Given a set* **T** *and a partial ordering* $\geq$ *on* **T**. *If* $\geq$ *satisfies the following condition (d), then* $\geq$ *is called a* ***total ordering***,

(d) *for any* $t_1, t_2 \in \mathbf{T}$, *we always have either* $t_1 \geq t_2$ *or* $t_2 \geq t_1$. ■

**Definition 1.7.** *Let* **T** *be a set, and* $\geq$ *be a partial ordering on* **T**. *Let* **S** *be a subset of* **T**. *If an element* $t \in \mathbf{T}$ *satisfies* $t \geq s$ *for all* $s \in \mathbf{S}$, *then the element t is said to be an* ***upper bound*** *of* **S**. *If for a given element* $t \in \mathbf{T}$, *the relation* $t_1 \geq t$ *implies* $t_1 = t$, *then the element t is said to be a* ***maximal element*** *of* **T**. ■

**Definition 1.8.** *Let* **T** *be a set, and* $\geq$ *be a partial ordering on* **T**. *Let* **S** *be a subset of* **T**. *If the restriction of* $\geq$ *to* **S** *is a total ordering of* **S**, *then* **S** *is said to be a* ***chain***. ■

Now we may state Zorn's lemma as follows,

**Zorn's lemma.** *Let* **T** *be a non-empty set and a partial ordering* $\geq$ *on* **T**. *If every chain of* **T** *has an upper bound, then there is a maximal element in* **T**. ■

**Discussion**

(1) Since Zorn's lemma is in fact an axiom for set theory, it can not be deduced from a simpler system of axioms.

(2) Zorn's lemma is a tool which helps us to simplify some proofs. Moreover, some results can only be deduced from Zorn's lemma. For instance, let us establish that in any bounded domain **D** of the real plane, there is always a maximal open disc. We shall use Zorn's lemma. Let **T** be the set of all open discs in the domain **D**. Let the usual set theoretic inclusion $\supseteq$ be the partial ordering. Then it is easy to establish that (1) the set **T** is non-empty. (2) let $\{\mathbf{D}_i : i \in \mathbf{I}\}$ be a chain, then $\bigcup_{i \in I} \mathbf{D}_i$ is obvious an open disc and hence an element in **T**, thus an upper bound of the chain. It follows from Zorn's lemma that there is a maximal element in **T** which is what we want. ■

## Exercises

(1) Let **Q**[x] be the set of all polynomials with rational coefficients. Prove that **Q**[x] is a countable set.

(2) Given any set **T**. Prove that the set theoretic inclusion $\supseteq$ is a partial ordering on the set of all subsets of **T**.

(3) Prove that the usual ordering $\geq$ is a partial ordering, and in fact a total ordering, for the set of all integers **Z**.

(4) Prove that the partial ordering in the above problem (2) satisfies the conditions of Zorn's lemma. Prove that the partial ordering in problem (3) does not satisfy the conditions of Zorn's lemma.

(5) Use the Mathematical induction to prove $1^2+2^2+\cdots+n^2 = (n(n+1)(2n+1)/3!)$.

(6) Let $\rho : S \rightarrow T$ be a map from the set S to the set T. Prove that $\rho$ is injective if and only if one of the following two conditions are satisfied;

(i) There exists a map $\tau : T \rightarrow S$, such that $\tau\rho =$ the identity map on $S$.

(ii) For any set U, and any two maps $\tau_1, \tau_2 : U \rightarrow S$, the relation $\rho\tau_1 = \rho\tau_2$ implies $\tau_1 = \tau_2$

(7) Let $\rho : S \rightarrow T$ be a map from the set S to the set T. Prove that $\rho$ is surjective if and only if one of the following two conditions are satisfied;

(i) There exists a map $\tau : T \rightarrow S$, such that $\rho\tau =$ the identity map on $T$.

(ii) For any set U, and any two maps $\tau_1, \tau_2 : T \rightarrow U$, the relation $\tau_1\rho = \tau_2\rho$ implies $\tau_1 = \tau_2$

## §2 Unique Factorization Theorem

The set of the natural numbers $\{1, 2, 3, \cdots\}$ will be called the set of the positive integers, denoted by $\mathbb{Z}_+$. The set of the integers $\{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$ will be denoted by $\mathbb{Z}$.

Mathematics originates from the natural numbers $\mathbb{Z}_+$. One way is to start with the *Peano's axioms* of the natural numbers and then introduce the four arithmetical operations, $+, -, \div, \times$. We can prove *the commutative laws, the associative laws* and *the distributive laws* thereafter in a logical manner. Using the natural numbers thus built, we may then construct the set of rational numbers $\mathbb{Q}$, the set of real numbers $\mathbb{R}$ and the set of complex numbers $\mathbb{C}$. For our readers, this logic method will be tedious and unnecessary. A portion of the necessary ingredients of those logic arguments is attached in an appendix (cf Appendix II Peano's axioms). We will assume that the reader is familiar with the arithmetical operations of $\mathbb{Z}, Q, R$ and C.

One of the most important operations in the theory of integers is the *long division algorithm*. This operation had been known to many ancient civilizations. In modern mathematics, it is known as the *Euclidean algorithm*[2,3]. Let us introduce the following concept,

**Definition 1.9.** *Let a be a real number. Let* $[a]$ *be the largest integer which is less then or equal to a.* ∎

[2] Euclid: Greek Mathematician lived at Alexandria, Egypt 306 B.C..

[3] The term 'algorithm' is a corruption of Persian algebraist al-Khwārizmi, 9th century.

**Discussion**

(1) The existence of $[a]$ is intuitively obvious, while equivalence to one of the fundamental properties of the real numbers, the ***Archimedean property***[4], which proclaims that for any two real numbers $n$ and $d > 0$, there exists a natural number $q$ with $q \cdot d > n$.

(2) For instance, $[3.1] = 3$, $[-3.2] = -4$ and $[5] = 5$. ▮

**Theorem 1.3. (Euclidean algorithm).** *Let $d$ be a positive real number and $n$ an arbitrary real number. Then there must be an integer $q$ and a real number $r$, such that*

$$n = q \cdot d + r, \qquad 0 \leq r < d$$

*Proof*: Let $q = [n/d]$, $r = n - q \cdot d$. Then we have

$$\begin{gathered} q \leq n/d < q + 1 \\ q \cdot d \leq n < q \cdot d + d \\ 0 \leq n - q \cdot d = r < d \end{gathered}$$

▮

**Corollary 1.** *In the above theorem, the numbers $q$ and $r$ are uniquely determined by $n$ and $d$.*

*Proof*: Let $q'$ and $r'$ be another pair of real numbers with

$$n = q' \cdot d + r'(= q \cdot d + r), \qquad 0 \leq r' < d$$

Then we have

$$(q - q') \cdot d = r' - r$$

We may assume that $q - q' \geq 0$. Then we get

$$0 \leq (q - q') \cdot d = r' - r \leq r' < d$$

Therefore we conclude

$$q = q', \qquad r = r'$$

▮

[4] Archimedes: Greek Mathematician and Scientist 287-212 B.C..

**Example 1**. *Using Euclidean algorithm, we may define the continuous fraction of any real number. Let us take an example; From* $\pi = 3.14159265358979 23846\cdots$, *we get*

$$\begin{aligned}
\pi = \frac{\pi}{1} &= 3 + \frac{0.14159265358979 23846\cdots}{1}\\
&= 3 + \cfrac{1}{\cfrac{1}{0.14159265358979 23846\cdots}}\\
&= 3 + \cfrac{1}{7 + \cfrac{0.00885142787144737 07\cdots}{0.14159265358979 23846\cdots}}\\
&= 3 + \cfrac{1}{7 + \cfrac{1}{\cfrac{0.14159265358979 23846\cdots}{0.00885142787144737 07\cdots}}}\\
&= 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{0.0088212355180831769\cdots}{0.00885142787144737 07\cdots}}}\\
&= 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{0.008851427871447\cdots}{0.000030192353364\cdots}}}}\\
&= 3 + \cfrac{1}{7 + \cfrac{1}{15 + \cfrac{1}{1 + \cfrac{1}{292 + \cdots}}}}
\end{aligned}$$

*Let us discard the decimal parts and only keep the integer parts in the above, and call the resulting rational numbers the partial continuous fractions. Then we get the partial continuous fractions of* $\pi$ *as follows,*

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

*The above rational numbers are 3, 22/7, 333/106, 355/113, 103993/33102. The first approximation, 3, was known to most ancient civilizations. The second approximation, 22/7, was due to Archimedes (250 B.C.) and is still used in high schools today. The third one was not very significant. The fourth one, 355/113 = 3.1415929203 ⋯, was very close to the true value of $\pi$, was discovered by Tsu Chhung-Chih (470 A.D.) in China and independently by Vieta (1593 A.D.) in France.*

*It is generally known in number theory that the partial continuous fractions are the best rational approximations with restrictions on the sizes of the denominators.* ∎

Another application of Euclidean algorithm is the unique factorization property of the integers **Z**. For this purpose, let us introduce,

**Definition 1.10**. *Let $a, b, c$ be integers. If $a = b \cdot c$. then we say that $a$ is a* **multiple** *of $b$ and $b$ is a* **divisor** *of $a$, in symbol, $b \mid a$. If $b \mid a_1, b \mid a_2, \cdots, b \mid a_n$, then we say that $b$ is a* **common divisor** *of $a_1, a_2, \cdots, a_n$. The greatest one among the common divisors of $a_1, a_2, \cdots, \alpha_n$ will be called the* **greatest common divisor**, *in symbol g.c.d., of $a_1, a_2, \cdots, a_n$. If $a_1 \mid b, a_2 \mid b, \cdots a_n \mid b$, then we say that $b$ is a* **common multiple** *of $a_1, a_2, \cdots, a_n$. The smallest non-negative integer which is a common multiple of $a_1, a_2, \cdots, a_n$ will be called the* **least common multiple**, *in symbol $\ell$.c.m. of $a_1, a_2, \cdots, a_n$.* ∎

**Theorem 1.4**. *Suppose that one of $a_1, a_2$ is non-zero. Then the greatest common divisor of $a_1, a_2$ is the smallest positive integer in the set* S=$\{b_1 \cdot a_1 + b_2 \cdot a_2 : b_i \in Z\}$. *We will use $(a_1, a_2)$ to denote the greatest common divisor of $a_1, a_2$.*

*Proof.* Let the smallest positive integer be $d = c_1 \cdot a_1 + c_2 \cdot a_2$. Applying Euclidean algorithm to the pair $d, a_1$, there exist $q_1$ and $r_1$ with

$$a_1 = q_1 \cdot d + r_1, \qquad 0 \le r_1 < d$$

If $r_1 \neq 0$, then we get

$$r_1 = a_1 - q_1 \cdot d = (1 - c_1 \cdot q_1)a_1 + (-c_2 \cdot q_1)a_2 \in \mathrm{S}$$

Note that then $r_1$ is a positive element in S which is less then $d$. A contradiction! We conclude that $r_1 = 0$, i.e.,

$$d \mid a_1$$

Similarly, we can prove

$$d \mid a_2$$

Namely, $d$ is a common divisor of $a_1$ and $a_2$. Let $d'$ be another common divisor of $a_1, a_2$. Then we have

$$d' \mid a_1, \quad d' \mid a_2 \Longrightarrow d' \mid c_1 \cdot a_1 + c_2 \cdot a_2 = d$$

Since $d$ is a positive integer, then we have $d \geq d'$. Therefore it follows from the definition that $d$ is the greatest common divisor of $a_1, a_2$. ∎

In the following we will establish the *unique factorization theorem* for $\mathbb{Z}$, which is sometimes called the *fundamental theorem of Arithmetics*. For this purpose, we will introduce the concepts of the *irreducible numbers* and the *prime numbers*. Note that in $\mathbb{Z}$ the only invertible elements with respect to multiplication are $1, -1$, i.e., if $n$ and $n^{-1}$ are both integers, then $n$ must be $1$ or $-1$.

**Definition 1.11.** *Let $a \neq 0, 1, -1$ be an integer. Then $a$ is said to be an irreducible number, if in any factorization of $a = b \cdot c$, for some integers $b$ and $c$, implies either $b = \pm 1$ or $c = \pm 1$. If for $f, g \in \mathbb{Z}, a \mid f \cdot g \Longrightarrow a \mid f$ or $a \mid g$, then $a$ is called a prime number.* ▮

**Lemma.** *In $\mathbb{Z}$, a number $a$ is an irreducible number if and only if it is a prime number.*

*Proof*: ($\Longrightarrow$) Let $a$ be irreducible. We may assume that $a$ is positive, otherwise replace it by $-a$. Suppose that we have

$$a \mid f \cdot g, \qquad f, g \in \mathbb{Z}$$

Suppose $a$ is not a divisor of $f$. Since $a$ is irreducible, i.e., the only positive divisors of $a$ are 1 and $a$, then the greatest common divisor of $a$ and $f$ must be 1. It follows from Theorem 1.2. that

$$1 = c_1 \cdot a + c_2 \cdot f$$

Multiplying by $g$ on both sides of the above equation, we get

$$g = g \cdot c_1 \cdot a + c_2 \cdot (f \cdot g)$$

Therefore we have $a \mid g$ and $a$ is a prime number.

($\Longleftarrow$) Let $a$ be a prime number and $a = b \cdot c$. Then we have $a \mid b \cdot c$ which implies $a \mid b$ or $a \mid c$, say $a \mid b, b = a \cdot d$. Trivially, we have $a = a \cdot (c \cdot d)$ and $1 = c \cdot d$. Therefore $c$ is multiplicatively invertible and must be 1 or $-1$. We conclude that $a$ is irreducible. ▮

**Discussion**

(1) For the general *rings* (cf Chapter III), the concepts of irreducible elements and prime elements are different. The coincidence of these two concepts establishes the Unique Factorization Theorem (see below).

(2) An expression $a = \prod_i p_i$ with all $p_i$ prime numbers will be called *a prime decomposition of $a$*. ▮

**Theorem 1.5. (Unique Factorization Theorem).** *Let $a > 1$ be any positive integer. Then $a$ has a prime decomposition $a = \prod_i p_i$. Moreover, all prime decompositions of $a$ are identical up to a reordering of $p_i$.*

*Proof*: We shall prove the existence and then the uniqueness of the prime decomposition. The present theorem is void for $a = 1$. Let us start with $a = 2$. Since 2 is a prime number, then the equation $2 = 2$ is a prime decomposition of 2. Let any positive integer $a > 2$ be given. Using Mathematical induction, we assume that any positive integer less than $a$ has