

數論初步

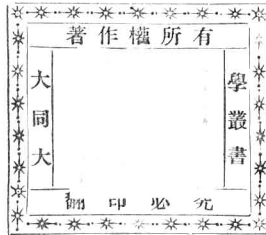
大同大學叢書

An Introduction to the Theory of Numbers

The Commercial Press, Limited
All rights reserved

大同大學叢書叢刊編輯部

胡敦復 朱香晚 華縮言 郁少華
葉上之 吳在淵 曹梁廈 胡憲生
胡剛復



中華民國二十年二月初版

大同大學叢書

數論初步

每册一元 商務印書館

編者	此進	天胡	在敦	淵復
校訂者	無錫	胡華	縮言	言
發行人	上海王	寶雲	山	路
印刷所	上海北河南路	印	寶山	五路
發行所	上海商務	印	中	市館
總發行所	上海商務	印	書	館

北平天津保定瀋陽吉林龍江濟南太原開封西安
南京杭州蘭谿安慶蕪湖南昌九江漢口長沙常德
衡州成都重慶廈門福州廣州潮州香港梧州雲南
貴陽張家口新嘉坡

商務印書館

數論初步

序

間嘗聞言：方今我國青年求知之慾甚於飢渴；私心竊喜，以爲學殖進步之速當可操券待矣。起視出版界，乃不禁爽然，小說出品，斗量車載；科學書籍，寥若晨星，其高深者尤難一二觀，是何也？商家本爲貨殖，供自應乎所求，陽春之和難求，資本時虞虛擲，卽有名作，未敢發行，而能載筆著述者又多寒士，腹笥雖富，僅足資生，知音之難，千古同慨，抱璞途泣，是其恆情，斯所以科學高深之作，絕跡於市也；然則奈何？曰：欲人多能知樂，必先使能操絃；欲人多能調羹，必先使能識味，青年求知之慾固在，必有以善導而養之，庶能充其量於正軌乎。

本書編輯之目的，卽在以整數論初步介紹於青年，力以平易爲主，凡理論之接近於高中數學程度者，儘量採用之。其較高部分，如代數、數等分、圓周問題、Galois 氏虛數、級數形式等，凡適當發展之各需有可觀之卷帙者概從割愛，每卷更附若干問題，以便初學之練習，學者倘能由此引起興趣而進求專書，則本書已不爲無補矣。

整數論一科，在實用方面尙無甚應用。此或與我國學界崇實主義之潮流不合。然數學之正軌，實在理論精嚴及運思深入，應用爲後起之事，今日無者他日或有，如昔之非歐幾里得幾何然，不足爲此科病也。

抑 Gauss 氏有言曰：「數學乃科學中之女王，而整數論又爲數學中之女王」，整數論之莊嚴映麗，儀態萬方，可於此語中得之。古來諸數學大家必有一時沉醉此中，則此科之價值從可知矣。

不佞粗疏讷陋，罣一漏萬，在所不免，甚望藉此拋磚引玉，得邦之彥碩有博大宏深之著作繼出爲幸。

中華民國十九年七月吳在淵識。

數論初步

目 錄

第一章 整數之初等性質

款	1. 基本概念及規律(例題一)	第1頁
	2. 約數及倍數, 單位(例題二)	3
	3. 素數,	7
	4. 素數之分佈(例題三)	9
	5. 歐氏之基本定理及算法(例題四)	13
	6. 整數之可約性(例題五)	20
	7. 析因數法定理,	23
	8. 約數之公式	26
	9. 完全數(例題六)	31
	10. 公約數及公倍數(例題七)	35
	11. 紀數法(例題八)	37
	12. 階乘數之析因數法(例題九)	40
	13. 尤氏函數	49

14.	尤氏函數之擴充(例題十).....	第 62 頁
15.	整式之析因數	69
	問題一	74

第二章 等餘之理論

16.	等餘式及其基本性質.....	81
17.	等餘式之類.....	85
18.	數列就法 m 之賡餘(例題十一)	92
19.	尤氏函數之別證(例題十二).....	100
20.	費氏定理	103
21.	費氏定理之應用(例題十三).....	112
22.	惠氏定理	116
23.	惠氏定理之應用.....	120
24.	蘭氏定理(例題十四).....	123
25.	循環小數之理論	126
26.	形式 $2^n \pm 1$ 之素數.....	135
	問題二.....	142

第三章 等餘式解法

27.	等餘式之種類.....	145
28.	一元一次等餘式.....	149

29. 聯立一元一次等餘式	第 155 頁
30. 一元高次等餘式	167
31. 屬於指數之數	172
32. 主根	176
33. 標數	184
34. 標數之應用	191
35. 二項等餘式	195
36. 雜例	200
問題三	206

第四章 平方賸餘

37. 賸餘及非賸餘	210
38. 羅氏之記號	211
39. 法爲合成數者之理論	214
40. 求法問題	225
41. 決定 $\left(\frac{-1}{p}\right)$	227
42. 哥氏定理	229
43. 決定 $\left(\frac{2}{p}\right)$	232
44. 互倒性律	235
45. 夏氏記號	243

46. 求法問題之解決	第 249 頁
問題四	255

第五章 不定方程式

47. 總論	257
48. 二元一次不定方程式	263
49. 多元一次不定方程式	271
50. $x^2 - Dy^2 = 1$ 之理論	278
51. 續論	290
52. $ax^2 + bxy + cy^2 = m$ 之解法	296
53. 普徧二元二次不定方程式	310
54. 劈氏數	316
55. 費氏問題	319
問題五	322

附 錄

(一) 約數表	325
(二) 標數表	327
(三) $x^2 - Dy^2 = 1$ 之最小正根表	331

數論初步

第一章 整數之初等性質

1. 基本概念及規律. 正整數,即

1, 2, 3, 4, 5, ……………

名之曰自然數. 本章所論為自然數之某種初等性質,為便利起見,當無混淆之慮時,恆用整數或數等語以表自然數.

吾人於此假定整數之意義,以及大於,小於,等於,和,差,積,等之意義,皆為學者所已知.

從如此所假定為已知之概念及定義可徑得下之諸定理:

定理一. 任意二整數之和為一整數.

定理二. 任意二整數之差為一整數.

定理三. 任意二整數之積為一整數.

其餘基本定理吾人所不必證者,包括之於下諸公式中:

定理四. $a+b=b+a.$

定理五. $a \times b=b \times a.$

定理六. $(a+b)+c=a+(b+c).$

定理七. $(a \times b) \times c = a \times (b \times c).$

定理八. $a \times (b+c) = a \times b + a \times c.$

此中 a, b, c 表任意自然數.

例 題 一

(1) 證下諸關係式:

$$1+2+3+\dots\dots\dots+n = \frac{1}{2}n(n+1),$$

$$1+3+5+\dots\dots\dots+(2n-1) = n^2,$$

$$1^3+2^3+3^3+\dots\dots\dots+n^3 = \left(\frac{1}{2}n(n+1)\right)^2 \\ = (1+2+3+\dots+n)^2.$$

(2) 求下各級數之和:

$$1^2+2^2+3^2+\dots\dots\dots+n^2$$

$$1^2+3^2+5^2+\dots\dots\dots+(2n-1)^2,$$

$$1^3+3^3+5^3+\dots\dots\dots+(2n-1)^3,$$

(3) 從諸方程式:

$$1^2=0+1, \quad 2^2=1+3, \quad 3^2=3+6, \quad 4^2=6+10, \dots\dots;$$

及諸方程式:

$$1=1^3, \quad 3+5=2^3, \quad 7+9+11=3^3, \quad 13+15+17+19=4^3,$$

.....:

發見及建設其規律。

2. 約數及倍數. 單位.

定義. 一整數 a 能以一整數 b 除盡之者, 謂有一整數 c , 能使 $a=bc$ 也。

從此定義, 顯然可知 a 亦能以 c 除盡。

二整數 b 及 c 謂為 a 之約數, 或曰因數, 而謂 a 為 b 或 c 之倍數。

求二整數 b 及 c 使 bc 等於一所設整數 a 之方法, 曰析因數法, 亦曰以 a 析成因數。

定理一. 若 b 為 a 之一約數, 及 c 為 b 之一約數, 則 c 為 a 之一約數.

因 b 為 a 之一約數, 則有一整數 β 使 $a=b\beta$. 因 c 為 b 之一約數, 則有一整數 γ 使 $b=c\gamma$. 以此 b 之值代入上一式中, 得 $a=c\gamma\beta$. 但從前款定理三, 知 $\gamma\beta$ 為一整數; 由是 c 為 a 之一約數, 而本定理已證明矣。

此定理亦可如下述之:

一數之約數亦為其倍數之約數, 或一數之倍數亦為其約數之倍數.

定理二. 若 c 為 a 及 b 二者之約數, 則 c 為 a 及 b 和或差, 即 $a\pm b$, 之約數.

從定理之假設, 知有二整數 α 及 β , 使

$$a = c\alpha, \quad b = c\beta.$$

加或減之，得

$$a \pm b = c\alpha \pm c\beta = c(\alpha \pm \beta) = c\delta.$$

此中 δ 爲一整數，由是 c 爲 $a \pm b$ 之約數。

定理三. 若 c 爲 a 及 b 之約數，又 p 及 q 爲任意整數，則 c 爲 $pa + qb$ 之約數。

證法與前定理之證相類，茲從略。

定理四. a 爲一整數，則一切整數恆可以如下諸式之一表之：

$$\underline{am, am+1, am+2, \dots, am+a-1.}$$

但此中 m 之值爲一整數。

設任取一整數爲 N ，則此 N 或爲 a 之倍數或非 a 之倍數，二者必居其一。若 N 爲 a 之倍數，則 N 可以 am 表之；若 N 非 a 之倍數，則在 N 中減去 a 之整倍數 am 以後必有小於 a 之賸餘，此賸餘必爲 $1, 2, 3, \dots, a-1$ 中之一，故 N 恆可以

$$am+1, am+2, \dots, am+a-1$$

之一表之。

觀察約數之方法. 在普通算術中有觀察約數之方法數事，今舉之於下，其證學者可自爲之：

(I) 凡數之一位數字爲 2 之倍數者，此數必有 2 之

約數

(II) 凡數之一位數字爲 5 之倍數者,此數必有 5 之

約數

(III) 凡數之十位及一位共二位數爲 4 之倍數者,此數必有 4 之約數.

(IV) 凡數之十位及一位共二位數爲 25 之倍數者,此數必有 25 之約數.

(V) 凡數之各位數字和爲 9 之倍數者,此數必有 9 之約數.

(VI) 凡數之各位數字和爲 3 之倍數者,此數必有 3 之約數.

(VII) 凡數中奇位數字和與偶位數字和之差爲 11 之倍數者,此數必有 11 之約數.

定義. 若 a 及 b 皆能以 c 除盡,則謂 c 爲 a 及 b 之公約數,或公因數

凡二個整數恆有一公約數 1.

能除盡 a 及 b 之最大整數名之曰 a 及 b 之最大公約數.
擴而充之,吾人可照此法定 n 個整數 $a_1, a_2, a_3, \dots, a_n$ 之公約數及最大公約數.

定義. 若一整數 a 爲二個或多個整數之倍數,則名 a 爲諸整數之公倍數.

一整數爲二個或多個整數之倍數而最小者爲其最小公倍數。

整數 1 爲一切整數之約數，爲一切整數約數之整數僅有此 1，此皆顯然可知者。名此 1 曰單位 (Unit)。

定義。 二個或多個整數除 1 外無公約數者名之曰互素 (to be prime to each other)。

定義。 若一組整數其中任意二數無 1 以外之公約數者，謂此一組整數互素。

例 題 二

(1) 若 n 爲正整數，證 $n^3 - n$ 可以 6 除盡之。

(2) 四個連續整數之積加 1，則其和爲一完全平方數。證之。

(3) n 爲正整數時，示 $2^{n+2} + 1$ 有一異於本身及 1 之因數。

(4) 一整數之平方必爲以下各形式之一：

$$(a) \quad 3m, \quad 3m+1;$$

$$(b) \quad 4m, \quad 4m+1;$$

$$(c) \quad 5m, \quad 5m \pm 1.$$

證之。

(5) 已知 $62 \times \times 427$ 爲 99 之倍數，求在 $\times \times$ 二位置

之數字。

3. 素數. 定義. 若一整數 p 與 1 異而除本身及 1 以外無他約數,則謂此數爲素數 (Prime number or Prime).

定義. 一整數至少有一個約數異於本身及 1 者謂之曰合成數 (Composite number or Composite).

於是,一切整數分成三類:

- (a) 單位;
- (b) 素數;
- (c) 合成數.

吾人已見第一類僅含一個數,第三類顯然含有無窮個數;由其含有 $2^2, 2^3, 2^4, \dots$ 即可見之.至次款中,吾人當見第二類亦含有無窮個數.

定義. 一合成數 N 可分成一雙因數 m, n , 即 $N = mn$, 則謂此 m 及 n 爲 N 之互補約數,或曰互補因數.

於是,素數僅有一雙互補約數爲其本身及 1, 即

$$N = 1 \cdot N.$$

合成數至少有二雙互補約數,如

$$N = 1 \cdot N = m_1 \cdot n_1 = m_2 \cdot n_2 = \dots$$

若 $1 < m_1 < m_2 < \dots$,

則 $N > n_1 > n_2 > \dots$.

故以 N 之約數依從小至大之次序列之,則可得

$$1 < m_1 < m_2 < \dots < n_2 < n_1 < N.$$

定義. 凡約數之爲素數者名之曰素約數,或曰素因數.

定理一. 凡大於 1 之自然數至少有一個素約數.

令 N 爲大於 1 之任意整數.

若 N 爲一素數,則 N 本身即爲其素約數.

若 N 爲一合成數,則必至少有二雙互補約數,如

$$N = 1. N = m_1. n_1 = \dots,$$

假定此中 $1 < m_1 < \dots < n_1 < N$,

即 m_1 爲 1 以外 N 之最小約數.然則 m_1 必爲 N 之素約數.何則,如云 m_1 爲合成數,則 m_1 必有比其本身小而非 1 之約數,而此約數亦必爲 N 之約數,則是 m_1 非 1 以外 N 之最小約數矣;與假定矛盾,不可也.

定理至此已證明矣.

定理二. N 爲任意整數, I 爲平方等於 N 之數(不必爲整數),若 N 無一小於或等於 I 之素因數,則 N 爲一素數.

假定 N 爲合成數, m, n 爲其任意一雙互補約數,而 $m < n$.

從定理之假設, $m > I$,

故必 $n > I$, 而 $m \cdot n > I^2$.

然 $I^2 = N$,

故 $m \cdot n > N$,

由是假定之 $N = m \cdot n$ 不合理.

故 N 必爲一素數。

4. 素數之分布. 希臘之愛拉託士細尼斯氏 (Eratosthenes)

有一檢出素數之法,可述之於下:

從 2 起,寫下各自然數列成一表.

2 爲一素數,在表中留此 2;從此後一數起數之,每逢第二個數即棄去,於是除 2 外,凡 2 之倍數皆棄去.

次,從 3 之後一數起數之,每逢第三個數即棄去.

再,從 5 起,棄去其後之各第五個數.

再從次一未棄之數——即 7——起,棄去其後之各第七個數.

以後累以此法進行,是曰愛氏之篩.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25

每次棄去之數於其頂上加點以識之,於是頂上無點者爲素數,頂上有一點者此數有一種素因數,頂上有二點者此數有二種素因數. 例如

$$\overset{\cdot}{25} = 5^2 \quad (\text{一種素因數 } 5)$$