科學文庫

第二集第一號

數論

呂竹人著

劉咸主編

中國科學社出版

中華民國二十七年六月

科學文庫

第二集第一號

數論

劉薇 編

中國科學社出版

中華民國二十七年六月

科學文庫

第二集　第一號

數論

中華民國二十七年六月初版

每冊實價國幣四角

編著者　呂　竹　人

主編者　劉　咸

發行者　中國科學社

發行人　楊　孝　述

印刷所　中國科學公司

上海福煦路六四九號

科學文庫緣起

近年以來,吾國朝野上下,迫於時勢需求,咸努力於救亡圖存之大業,而科學建設因相需之殷,進行尤不遺餘力,於是國人對於科學知識之追求,異常迫切,此誠一良好現象也.顧坊間之出版物,雖汗牛充棟,名目繁多,然求其能供給學術資料,作知識上之啓發者,則寥寥可數,而介紹近代科學,具有眞實價值之"硬性"刋物,尤屬鳳毛麟角,有識之士未嘗不引以爲憾焉!

本社爲吾國先進科學團體,以提倡科學研究,傳播科學知識爲職志,秉一貫政策,循序漸進,不激不隨,不偏不黨,不矜功能,不趨時尙,二十年來,漸爲社會人士所認識,今後仍當本此方針,以求邁進,格物致知,利用厚生,期於國計民生,有所裨益.

當本社成立伊始,首先發行科學雜誌以爲傳播科學知識之「機關」,日積月累,現已刋行二十餘卷,就前二十卷之內容約略統計,得科學專著論文二千二百三

十餘篇,給科學新聞,書報介紹,論文提要,拾零,雜俎,通信,來件等,都三萬二千零四十八頁,期能集國人介紹科學文字之大成,亦即本社倡導科學之些許成績(本社研究成績另有論文專刊,研究叢刊及生物論文等,不在此例).彌足珍貴,就中有不少論文為極精構之作,具有永存價值;惟因各卷期印數有限,且歷時既久,多已絕版,致使有心購讀者,徧覓無由,良以為憾.茲為應國人迫切需求起見,爰分門別類,彙編重刊,發行單印本,擬定文庫內容系統如下:

第一集: 科學通論,科學史,科學名人傳記.

第二集: 數學,天文學.

第三集: 物理學,化學.

第四集: 地理學,氣象學,地質學,礦物學.

第五集: 動物學,植物學,古生物學.

第六集: 人類學,考古學.

第七集: 醫藥科學.

第八集: 農林科學.

第九集: 工程科學.

第十集: 社會科學.

以上略依現代科學分類法,細分十類,每類為一集

每集之內視材料多寡性質異同分別輯成小冊子每冊為一號各集自為號序不相混雜更不限定時間完成文庫之全部但視人力財力所能及陸續分別出版如此各門學科分之可自成獨立之一系合之則為科學全部大體系所以便圖書館之收藏與科學家之採覽焉.

劉 咸.

上海中國科學社編輯部.

數　論

目　次

數論

第二章*

緒論

§§1. 1. 數數之二名所包至廣自首出之自然數以至近人所發現之超越數靡不統攝於其中故二言數論已足以囊括算學之全部而有餘蓋不惟代數分析以數爲宗，即形學力學既憑精確之標以爲研討，亦不能須臾離數也. 然而數論一科在習慣上實僅以整數爲題材而論域復限於整數本身，其引伸旁及之義，如戴德金氏之分割說等，皆在所非議，故數論者算學之一枝，以考論整數本身之性質爲事者也.

§§2. 2. 整數分兩大類，曰素數(prime numbers)，曰非素數，又曰複數((composite numbers)). 後者可以大於一之他數除盡，無餘；前者自一及本數外無他數可以除盡.

凡偶數除2外皆爲非素數，奇數中既爲素數，既爲非素數，得依下法決擇.

---

*原載科學第15卷第10,11期.

依自然順序書若干奇數,如

1	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

其第一數 1 爲素數,置勿論.第二數 3 亦爲素數,自 3 以後,每間二數如 9,15,21,27,39 等皆爲 3 之倍數,各加一點於上以爲記.考 3 後未加點之第一數爲 5,此必爲素數.自 5 以後,每間四數如 15,25,35,45,等皆爲 5 之倍數,亦各附一點於上以爲記.再考 5 後未加點之第一數爲 7, 7 亦必爲素數.自 7 以後,每間六數又皆爲 7 之倍數.一般,若前 n 個素數之倍數皆已加點,則第 $n+1$ 個未加點之數必又爲一素數,否則該數可以前 n 個素數中之一二整除,應已加點.設該數爲 p,則自 p 以後,每間 $p-1$ 數必皆爲 p 之倍數,卽 $3p,5p,7p,\cdots\cdots$ 此又當附點標明.逐次如此,卽得甚多之奇素數.

凡非素數,析爲二因子,必有一不大於其平方根.故欲考某數以下之奇素數,只須將該數平方根以下諸素數之倍數一一加點,餘未加點之數必皆爲素數無疑,是

爲上法實施時之一助.

定理一　素數之數爲無限多.

假如素數爲有限多,其中必有一最大之素數 p. 自 p 以下諸素數,均在 1.2.3.……p 之中,故皆能除盡 $p!$, 皆不能除盡 $p!+1$. 此若爲素數,則是有一素數大於 p; 此若非素數,則其素因子亦必大於 p, 是仍有一素數大於 p. 皆與 p 爲最大素數之說相違,故知素數之數必不能爲有限多.

本定理據云爲歐几里得氏所發現,後經戴力歇來(Dirichelet)氏推廣爲

定理二　設 a 與 d 不能以同一數除盡,則

$$a, a+d, a+2d, \cdots\cdots a+rd,$$

一宗數中之素數爲無限多.

證此定理,須用解析方法,卽借助於無窮級數.其說頗難明瞭,茲不縷述.惟除定理一外,此中尙有一二特例專端,如 (*i*) $4h-1$ 形之素數爲無限多, (*ii*) $6h-1$ 形之素數爲無限多等,則亦易於證明.如欲證(*i*),則可假定 $4h-1$ 形之素數僅有 $p_1, p_2, p_3, \cdots\cdots p_n$, 其中最大者爲 p_n. 考

$$N=4\,p_1p_2\cdots\cdots p_n-1$$

一數,亦爲 $4h-1$ 之形,而不能以 $p_1p_2\cdots p_n$ 中之任何數除

盡若N爲素數則$p_1, p_2, \cdots, p_n$是有一$4h+1$形之素數大於p_n若N非素數則必有若干素因子其形爲$4h+1$或$4h-1$但不能皆爲$4h+1$否則N之形亦將爲$4h+1$與書實相矛盾故N至少有一素因子其形爲$4h-1$此因子必大於p_n可知$4h-1$形素數爲有限多之假定於理不合依類似之方法亦可證明$6h-1$形之素數爲無限多.

算學家嘗欲求得一代數式僅產素數然迄無成凡有理整代數函數皆不能僅產素數因$f(a)$若爲一素數$=p$則$f(a+mp)$必非素數由爾瑪氏(Fermat)嘗自謂得之於

$$2^{2^{2^n}}+1.$$

此式於$n=0,1,2,3,4$時得素數

$$3, 5, 17, 257, 65537.$$

但尤拉氏(Euler)考得$n=5$時,

$$2^{2^{2^n}}+1=641\times 6700417$$

此不爲素數.

§§ 33. 一數同時爲m個數之因子,謂之諸m數之公因子.公因子中之極大者,曰最大公因子.兩數無大於一之公因子,謂之互素,亦云互爲素數(prime to each other).

一數c爲a, b兩數之公因子,亦必爲$la+mb$之一

因子,其l與m為任何(正或負)整數.由c既為a,b之因子,必有兩數a',b'合於等式

$$a=a'c \qquad b=b'c$$

故 $$la+mb=la'c+mb'c=(la'+mb')c$$

即c可以除盡$la+mb$.

緣此一義,遂有歐几里得氏求兩數最大公因子之成法:設兩數為A與B,且設$B<A$.以B除A,命其商為Q,其殘為$R_1<B$,得

$$A=QB+R_1 \cdots\cdots\cdots\cdots(1)$$

即 $$A-QB=R_1 \cdots\cdots\cdots\cdots(1)$$

若$R_1=0$,則A與B之最大公因子即為B;若$R_1\neq 0$,則以R_1除B,命其商為Q_1,其殘為$R_2<R_1$,又得

$$B=Q_1R_1+R_2 \cdots\cdots\cdots\cdots(2)$$

假定$R_2\neq 0$而以R_2除R_1,命其商為Q_2,其殘為$R_3<R_2$,即又得

$$R_1=Q_2R_2+R_3 \cdots\cdots\cdots\cdots(3)$$

逐次如是,因餘數遞減,至某階段必$R_{n+1}=0$,而R_n能除盡R_{n-1}.故

$$R_2=Q_3R_3+R_4 \cdots\cdots\cdots\cdots(4)$$

$$\vdots \qquad \vdots \qquad \vdots$$

$$R_{n-2}=Q_{n-1}R_{n-1}+R_n \cdots\cdots\cdots\cdots(5)$$

$$R_{n-1}=Q_n R_n \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots (6)$$

從 (1) 式,知 B 與 R_1 之公因子必爲 A 之一因子;從 (1′) 式,又知 A 與 B 之公因子必爲 R_1 之一因子.故 A,B 之最大公因子與 B,R_1 之最大公因子相同.若命兩數 A,B 之最大公因子爲 $D(A,B)$,此可書爲

$$D(A,B)=D(B,R_1)$$

由 (2)(3)(4) 諸式,又得

$$\begin{array}{ccc} D(B,R_1) & = & D(R_1,R_2) \\ \vdots & & \vdots \\ D(R_{n-2},R_{n-1}) & = & D(R_{n-1},R_n) \end{array}$$

最後, $D(R_{n-1},R_n)=R_n$

故 $R_n=D(A,B)$

而 A,B 之最大公因子卽爲 R_n.

逐次所得之餘數,皆可化爲 $lA+mB$ 之形,由 (1′) 式,見

$$R_1=l_1A+m_1B$$

以 R_1 之值代入 (2) 式,得

$$R_2=l_2A+m_2B$$

再以 R_1 及 R_2 之值代入 (3) 式,又得

$$R_3=l_3A+m_3B$$

終至 $R_n=l_nA+m_nB$

當A與B互爲素數,其最大公因子爲1,此式又化爲

$$1=l_nA+m_nB.$$

由是得

定理三. 若A與B兩數之最大公因子爲D,則必有兩數l,m令

$$lA+mB=D \quad \cdots\cdots(7)$$

定理四 若A與B兩數爲互素,則必有兩數l,m令

$$lA+mB=1 \quad \cdots\cdots(8)$$

從本定理,知l,m兩數之存在爲A,B互素之必要條件.但亦易知其爲圓滿條件,因據(8)式,能除盡A,B之數亦必能除盡1.

合於(7)(8)兩式之l,m得有無限多.$l=l_1, m=m_1$能合,則$l=l_1+kB, m=m_1-kA$亦能合,其k爲任何整數.在此兩式,l,m正負顯不相同,命k取適當之正負值,可任使其中之一爲正,餘一爲負.

§4. 由上節中之(7)式,知兩數之任一公因子必爲其最大公因子之一因子.故三數以上之最大公因子亦得仍用前法分若干步求之.例如有n個數$A_1,A_2,\cdots\cdots A_n$,則先求A_1,A_2之最大公因子D_1,次求D_1與A_3之最大公

因子 D_2，復次求 D_2 與 A_4 之最大公因子 D_3，繼續為之，至達 D_{n-2} 之最大公因子 D_{n-1}。此最後之 D_{n-1} 為 n 個數之一公因子，甚明．論而察之，又知其即為此 n 個數之最大公因子．因 $A_1, A_2, \ldots\ldots, A_n$ 之任一公因子必為 $D_1, A_3, \ldots\ldots, A_n$ 之一公因子，亦即為 $D_2, A_4, \ldots\ldots, A_n$ 之一公因子，亦即為 $D_3, A_5, \ldots\ldots, A_n$ 之一公因子．依此類推，知其亦為 D_{n-1} 之一因子．

在三數以上之場合，亦有與(7)(8)相類之式．此可用遞推法證明之．蓋 $A_1, A_2, \ldots\ldots, A_n$ n 個數之最大公因子 D_{n-1}，即為 $A_1, A_2, \ldots\ldots, A_{n-1}$ 之最大公因子 D_{n-2} 與 A_n 之最大公因子，是必有兩數 l, m 合

$$lA_n + mD_{n-2} = D_{n-1}$$

若在 $n-1$ 個數 $A_1, A_2, \ldots\ldots, A_{n-1}$ 之場合，恆有 $n-1$ 數 $h_1, h_2, \ldots\ldots, h_{n-1}$ 合

$$h_1A_1 + h_2A_2 + \cdots\cdots + h_{n-1}A_{n-1} = D_{n-2}$$

則以 D_{n-2} 之值代入前式，即知在 n 個數 $A_1, A_2, \ldots\ldots, A_n$ 之場合，亦恆有 n 數 $k_1, k_2, \ldots\ldots, k_n$ 合

$$k_1A_1 + k_2A_2 + \cdots\cdots + k_nA_n = D_{n-1}$$

但在兩數 A_1, A_2 之場合，必有兩數 h_1, h_2 合

$$h_1A_1 + h_2A_2 = D_1$$

故存在三與數 A_{11}, A_{12}, A_{13} 之場合，必有三數 $k_{11}k_{12}k_{13}$，俾

$$k_{11}A_{11}+k_{12}A_{12}+k_{13}A_{13}=D_2$$

推之存在 m 個與數 $A_{11}, A_{12}, \cdots\cdots A_{1n}$ 之場合，亦必有 m 個數 $l_{11}, l_{12}, \cdots\cdots l_{1n}$ 俾

$$l_{11}A_{11}+l_{12}A_{12}+\cdots\cdots+l_{1n}A_{1n}=D_{n-1}\cdots\cdots(99)$$

設此 m 個與數無大於 1 之公因子，則(99)式又化爲

$$l_{11}A_{11}+l_{12}A_{12}+\cdots\cdots+l_{1n}A_{1n}=1\cdots\cdots(100)$$

§§55. 定理五. 若 a 與 bc 爲互素，而能除盡 abb，則 cc 必能除盡 bb.

a 與 c 爲互素，依定理四必有兩數 l, m 俾

$$1=la+mac.$$

兩端各乘以 l，則

$$bb=labb+mbbc.\cdots\cdots(101)$$

c 能除盡 $labb$，又能除盡 $mbbc$，故必能除盡 bb.

上(101)式實又證明

定理六. 若 a 及 bb 各與 cc 爲互素，則 abb 與 cc 亦必爲互互素. 因一數能除盡 abb 及 cc，須能除盡 bb. 從此本定理，而直得

系一. 若 $a, b, \cdots\cdots k$ 各與與數 m 爲互素，則 $abb\cdots kk$ 亦必與 m 爲互素. 由此及定理五，又得

系二. 若$a, b, \cdots k$各與m爲互素,而m能除盡$ab\cdots kl$,則m必能除盡l.

定理五又可用下之方法證之:—

依假定,a與c爲互素,而c能除盡ab. a可視爲小於c,否則以c除a,得商q,必有餘數$d\neq o$與c爲互素且小於c,而

$$ab=(qc+d)b$$

$$bd=ab-bcq$$

卽c仍能除盡bd.

a小於c,則可以a除c,命其商爲n其餘數爲$a_1<a$,得

$$c=na+a_1$$

卽

$$a_1=c-na$$

其$a_1\neq o$,且與c爲互素.兩邊乘以b,則

$$a_1b=bc-nab$$

c能除盡bc及nab,必能除盡a_1b,但$a_1<a<c$.

用同法,可再得一數$a_2<a_1$,而c仍能除盡a_2b.繼此又可得$a_3, a_4, \cdots\cdots$諸a遞減而不能爲零,終必爲1. 故知c必能除盡b.

§ 6. 一數同時爲n個數之整倍數,謂之該n個數之公倍數.公倍數之極小者,曰最小公倍數.