

数论简明教程

〔苏联〕Л. Я. 奥库涅夫著

科学技术出版社

数 論 簡 明 教 程

〔苏联〕Л. Я. 奥庫涅夫著

洪 波 譯

科 学 技 術 出 版 社

內 容 提 要

本書系根据苏联 Л. И. 奥庫涅夫教授所著的“数論簡明教程”譯出,原書經苏联教育部審定为师范大学的参考書,書中內容分:整数的整除性理論,連分数基本理論,数論函数,同余式,含有未知数的同余式,元根和指标等六章。

本書可作为綜合性大学及师范学院数学系整数論的教本或参考書,也可供自修数論的讀者及中学教师作参考閱讀之用。

3200/50

数 論 簡 明 教 程

КРАТКИЙ КУРС ТЕОРИИ ЧИСЕЛ

原 著 者 [苏联] Л. И. Окунев

原出版者 УЧПЕДГИЗ • 1956 年版

譯 者 洪 波

*

科学技術出版社出版

(上海南京西路 2004 号)

上海市書刊出版業營業許可証出 079 号

上海启智印刷厂印刷 新華書店上海發行所总經售

*

統一書号: 13119 • 120

开本 850×1168 耗 1/32 印張 6 13/16 • 字数 165,000

1958 年 3 月第 1 版

1958 年 3 月第 1 次印刷 • 印数 1—2,700

定价 (10) 1.40 元



序 言

我是遵照着师范大学数学物理系整数論的教学大綱來編寫這本書的。書中有相当多数量的習題, 可以作为計算的性質, 也可以作为理論的性質。書中的末尾刊載了某一些習題的提示和解答。

Л. Я. 奧庫涅夫

1955 年 11 月 26 日

譯 者 的 話

這本書是奧庫涅夫教授根據蘇聯師範大學整數論教學大綱編寫的，它的內容淺出深入，很宜於作為我國師範學院整數論一課的教科書。

書中的內容以解析數論的基本知識為主，但也介紹了一些代數數論的基本概念，特別，書中以理想子環的概念來討論最大公約數，使得一些問題更便於理解。

本書對於連分數的基本理論介紹得很詳細，因而在超越數方面的材料，也談得很多。對於素數分布問題本書有着豐富的內容，而且还介紹了有名的車比雪夫不等式。這些都是本書的特點。

由於本書是蘇聯的教科書，所以作者對蘇聯及俄國數學家在數論上的成就，介紹得很多。如果用來作為我國的教材，那還需要補充以我國古代的以及現在的（如陳子、孫子、劉徽、秦九韶、朱世傑、李詒……華羅庚）數學家數論方面的成就。

書中一部分的習題（特別是在書末附有解答的），可以作為家庭作業，也可以作為教材來處理。

最後，希望讀者們對於譯文提出指正和批評！

洪 波

1957年9月25日

目 錄

序 言	1
譯者的話	2
第一章 整数的整除性理論	1
§ 1. 整除性的概念及其最簡單的性質	1
§ 2. 數環、理想子環	4
§ 3. 整數環中的理想子環、最大公約數	6
§ 4. 欧几里得輾轉相除法	12
§ 5. 素數、整數的素因子分解式、爱拉托斯散納篩子	14
§ 6. 最小公倍數	20
§ 7. 整除性理論發展史漫談	22
第一章的習題	25
第二章 連分數基本理論	28
§ 8. 有限連分數	28
§ 9. 近似分數的基本性質	33
§ 10. 無限連分數	39
§ 11. 拉格蘭日定理	46
§ 12. 近似分數作為無理數的近似值	51
§ 13. 超越數	59
第二章的習題	71
第三章 數論函數	74
§ 14. 函數 $[x]$	74
§ 15. 欧拉函數	76
§ 16. 茂別烏斯函數	84
§ 17. 素數在自然數列中的分布	87
第三章的習題	105

第四章 同余式	109
§ 18. 同余式, 基本性質	109
§ 19. 同余的數類	112
§ 20. 歐拉和費爾馬定理	120
第四章的習題	122
第五章 含有未知數的同余式	124
§ 21. 一個未知數的同余式的解答	124
§ 22. 一次同余式	128
§ 23. 一個未知數的同余式組	133
§ 24. 一個未知數的高次同余式	139
§ 25. 含有未知數的對於素數模的同余式	142
§ 26. 二次同余式、勒讓德符號	148
§ 27. 約可比符號	160
§ 28. 多個未知數的同余式	166
§ 29. 對於素數模的多個未知數的一次同余式組	170
第五章的習題	174
第六章 元根和指標	180
§ 30. 一數對於某一模的指數	180
§ 31. 元根	183
§ 32. 指標	187
§ 33. 指標表	189
§ 34. 利用指標表來解二項同余式	191
第六章的習題	192
一些習題的提示和解答	196
指標表	205
參考書籍	211
譯名對照表	212

第一章

整数的整除性理論

§ 1. 整除性的概念及其最簡單的性質

数論最基本的任务就是研究整数的性質。不过，数論中許多重要的問題，都要直接地或者間接地牽涉到数的整除性概念。因此，在我們教程的开端，要先來叙述一些整数整除性的基本理論。教程的極大部分提供了同余式的理論，这可以作为整除性理論的延續。

数論的創始人之一，有名的学者欧拉，在俄國住了三十年左右。此后，在数論的發展上，俄國的学者起着首要的作用。我們只要提出上一世紀俄國偉大的数学家 И. Я. 車比雪夫所創立的数論学派就够了，按本身的作用來說，这学派在全世界是唯一的。苏联的学者們在这方面起着主導作用，而且在最近的三十年間，院士 И. М. 維諾格拉陀夫和他的学派得到了更巨大的主要結果。在我們的教程里，对于数論範圍內的成就，無論是俄國的或者是苏联的学者的，我們都給以相當的地位。

現在，讓我們回到整数整除性理論上去。假設 a 和 b 是任意整数，如果存在第三个整数 c ，使得 $a = bc$ ，那么我們說， a 是 b 的倍数，或者 a 被 b 整除，而 b 整除 a 。今后，为簡單起見，我們用符号 b/a 來表示，意思就是， b 整除 a 。这样一來，我們有 $2/4$ ，但 $3 \nmid 4$ ； $0/0$ ，但 $0 \nmid a$ ，当 $a \neq 0$ 时。顯然，假使 b/a ，那么 $\pm b/\pm a$ 。

我們要指出整数整除的一些性質。

- 1°. a/a 及 $1/a$, 其中 a 是任意整數.
- 2°. 假使 a/b , 及 b/a , 那麼 $a = \pm b$.
- 3°. 假使 b/a 及 c/b , 那麼 c/a (傳遞性).
- 4°. 假使 c/a , c/b , 那麼 $c/a \pm b$.
- 5°. 假使 c/a , 那麼 c/ab .

性質 1° 是顯然的。數目 a 的因子 ± 1 和 $\pm a$, 為了區別於其他因子起見, 有時我們叫他為平凡因子。性質 2° 可用下面方法導出。根據 a/b 和 b/a 的整除條件, 我們得到

$$b = aq$$

和

$$a = bq_1,$$

其中 q, q_1 是整數。把第二個等式中的 b 值用第一個等式中的來代替, 我們求得 $a = aqq_1$ 。現在, 假使 $a \neq 0$, 那麼, 約去 a , 得到 $qq_1 = 1$, 因此 q 和 q_1 都要等於 ± 1 (因為 q 和 q_1 是整數)。所以 $a = \pm b$ 。當 $a = 0$ 時, 關係式 $a = \pm b$ 是顯然的, 因為條件 $0/b$ 只有在 $b = 0$ 時才可能。

性質 3° 可以這樣地導出。假使 b/a 及 c/b , 那麼

$$a = bq_1 \quad (1)$$

及

$$b = cq_2, \quad (2)$$

其中 q_1, q_2 是整數。把等式 (2) 中的 b 值代入等式 (1) 中, 我們得到: $a = cq_1q_2$, 或 $a = cq$, 其中 $q = q_1q_2$, 是一整數。因此推出 c/a 。

性質 4° 和 5° 可以模仿性質 2° 和 3° 來推出。

下面的定理在整數整除性理論中起着重要的作用。

關於帶余數除法的定理。假使 a 和 $b > 0$, 且都是整數, 那麼我們總可以選取這樣一對整數 q 和 r , 使得: 1) $0 \leq r < b$; 2) $a = bq + r$, 而且 q 和 r 是唯一確定的。

附注 數目 q 叫做不完全商數, r 叫做 a 被 b 除的余數。為了簡單起見, 我們可以把 q 叫做商數, 省掉“不完全”這些字。

證明 我們來研究 bx 這一式子, 其中 x 可給以一切可能的整

数值,可以是正的,也可以是負的。当 x 增加时,顯然, bx 的值也是增加的。因而,可以在某一整数 $x=q$ 时,我們有 $bq \leq a$, 而在 $x=q+1$ 时,就有 $b(q+1) > a$. 我們用 r 來表示差数 $a-bq$. 由不等式 $bq \leq a$ 和 $b(q+1) > a$ 可以推出 $a-bq \geq 0$ 和 $b > a-bq$, 即 $r \geq 0$ 和 $r < b$. 这样一來, $0 \leq r < b$. 其次,由等式 $r = a-bq$ 可以推出 $a = bq + r$. 定理的第一部分已經証明了。

唯一性这一部分我們利用反証法來証明。假定除了 q 和 r 以外,还有別的商数 q_1 和余数 r_1 . 于是

$$a = bq + r, \quad (3)$$

$$a = bq_1 + r_1, \quad (4)$$

而且 $0 \leq r < b$, $0 \leq r_1 < b$. 由等式(3)减去等式(4),我們得到:

$$b(q - q_1) + (r - r_1) = 0. \quad (5)$$

假定 $r \neq r_1$; 为确定起見,設 $r > r_1$. 于是 $0 < r - r_1 < b$. 現在我們來看等式(5),它可以化成下面的等式:

$$b(q - q_1) = -(r - r_1).$$

上面等式的左边部分是 b 的倍数,因此右边部分也應該是 b 的倍数,即 $b | r - r_1$. 但差数 $r - r_1$ 不可能是 b 的倍数,因为 $r - r_1$ 是一个小于 b 的正整数。所以, $r \neq r_1$ 的假定是不正确的,因而 $r = r_1$, 也就有 $q = q_1$.

剛才定理的証明还可以推廣到 b 是負整数的情况上去,也就是:假使 $b < 0$, 那么 $b = -|b|$. 另一方面,应用帶余数除法定理,对于 b 的絕對值 $|b|$, 我們有: $a = |b| q_1 + r$, $0 \leq r < |b|$. 因此有 $a = bq + r$, 其中 $q = -q_1$.

所以,假使 b 是不等于零的任意整数(正的或負的),那么,永远可以选取这样一对整数 q 和 r , 使得: 1) $0 \leq r < |b|$; 2) $a = bq + r$. 同时, q 和 r 是唯一确定的。

推論: 当而且只当 a 被 $b (b \neq 0)$ 除的余数等于零时, 整数 a 被整数 b 所整除。

事实上, 当 $r=0$ 时, 等式 $a=bq+r$ 变成 $a=bq$, 因此 b/a . 反过来, 假使 a 是 b 的倍数, 那么等式 $a=bc$ 应该成立, 其中 c 是某一整数。因此, 根据商数和余数的唯一性, 可以得到 $c=q$, 而余数 r 等于零。

§ 2. 数环、理想子环

假使利用环和理想子环的概念, 那么今后整数整除性的说明会更加嚴整而且普遍化。

在上一節的討論中, 我們應該注意到, 整数的和, 差及積也是一个整数。整数所具有的这一种性質, 我們可以叫它为: 关于算術运算加法, 减法及乘法的关闭性。不过, 关于这些运算的关闭性, 对于别的許多数集也是成立的。我們來举出一些例子。

例子 1. 所有偶数的集合关于加法、减法及乘法是关闭的(数目 0 是作为偶数的!), 不过, 奇数的集合只关于乘法是关闭的。

2. 我們來研究形如 $a+b\sqrt{2}$ 的实数集合, 其中 a, b 是任意整数。两个数目 $a_1+b_1\sqrt{2}$ 及 $a_2+b_2\sqrt{2}$ 的相加或相减可以得到同样形式的数目: $a+b\sqrt{2}$, 其中 $a=a_1\pm a_2$, $b=b_1\pm b_2$ 都是整数。同样地, $a_1+b_1\sqrt{2}$ 及 $a_2+b_2\sqrt{2}$ 二数的相乘也可以得到同样形式的数, 其中 $a=a_1a_2+2b_1b_2$, $b=a_1b_2+a_2b_1$ 都是整数。这样一來, 我們所研究的数集关于加法、减法和乘法是关闭的。

3. 容易驗証, 复数 $a+bi$ (i 是虛数單位, a, b 是整数) 的集合关于加法、减法及乘法是关闭的。順便說一句, a, b , 是整数的数目 $a+bi$, 通常叫做复整数或高斯整数。

所有这些例子引進了下面这一重要的概念。

定义 1°. 数集 M , 假使它关于前三个算術运算(加法, 减法及乘法)是关闭的, 那我們就叫它为数环。

这样一來, 偶数集構成一数环, 全体形如 $a+b\sqrt{2}$ (a, b 是整数) 的数及全体高斯整数也是数环。

关于定义 1° 我們要作一些說明：

1. 任何数环必包含数目 0. 事实上, 假使 a 是数环 M 中的任意一数, 那么差数 $a-a=0$ 也应该属于 M .

2. 任何数环 M 中若含有数目 a , 那么一定又含有其相对数 $-a$. 事实上, 因为数目 a 和 0 属于 M , 那么它的差数 $0-a=-a$, 也应该属于 M .

3. 由一个数目 0 所构成的数集, 我們有权把它当作数环来討論. 事实上, $0 \pm 0 = 0$, $0 \cdot 0 = 0$.

可能有这样的事情, 数环 M 中, 除了零以外, 别的数目关于第四种运算——除法(当然, 除了用零去除以外)是关闭的, 这样的数环叫做**数体**. 例如全体实数是一数体, 全体有理数是一数体. 相反地, 所有高斯整数集合只是数环, 而不是数体, 因为除法会使它超出这集合的范围——两个高斯整数的商可能不是高斯整数. 例如, $\frac{i}{2i} = \frac{1}{2}$. 不过, 复数集合 $a+bi$, 其中 a, b 是有理数, 也构成一数体^①. 顯然, 最大的数体是所有复数的集合.

定义 2°. 数环 M 中的部分集合 A , 假使具有下列性質: 1) A 的全体也构成一个数环; 2) 集合 A 中的任意一数乘以数环 M 中的任意数时, 得到一个也属于集合 A 的数, 那么它可以叫做数环 M 中的**理想子环**.

例子 1. 我們已知, 全体偶数构成一数环. 此外, 当一偶数乘以任意整数时, 永远得到偶数. 所以, 全体偶数是整数环的理想子环.

2. 由一个零构成的集合是任一数环 M 的理想子环. 这是由于: a) 所說的集合是一个数环; b) 当零乘以任意数时也得到零. 这个理想子环以后我們叫它零理想子环, 而用 (0) 来表示.

3. 我們來研究全体形式如 $6m+9n$ 的数目, 其中 m, n 通过

① 这个数体叫高斯有理数体。

一切可能的整数值。我們用 $(6, 9)$ 來表示这个数集, 而且要証明它是整数环中的理想子环。

假設 $a=6m_1+9n_1$ 和 $b=6m_2+9n_2$ 是集合 $(6, 9)$ 中的任意二数。于是

$$a \pm b = 6m' + 9n', \quad ab = 6m'' + 9n'',$$

其中 $m' = m_1 \pm m_2, n' = n_1 \pm n_2, m'' = 6m_1m_2 + 9m_1n_2 + 9m_2n_1, n'' = 9n_1n_2$ 都是整数。这一切說明了前面三个算術运算是不会超出集合 $(6, 9)$ 的範圍的, 即, $(6, 9)$ 是一个数环。其次, 假設 r 是任意整数, 把 $a=6m_1+9n_1$ 乘以 r , 我們得到同样形式的式子: $ar=6m+n$, 其中 $m=m_1r, n=n_1r$ 都是整数。这样一來, 集合 $(6, 9)$ 是整数环中的理想子环。

一般地, 假設 $a_1, a_2, \dots, a_k$ 是数环 M 中的一組数目。我們用 $(a_1, a_2, \dots, a_k)$ 來表示全体形如 $a_1m+a_2n+\dots+a_kt$ 的数目, 其中 $m, n, \dots, t$ 通过数环 M 中的一切可能值。借助于类似的論断, 我們不难証明集合 $(a_1, a_2, \dots, a_k)$ 是环 M 中的理想子环, 通常我們叫它为由数目 $a_1, a_2, \dots, a_k$ 生成的理想子环。也有这样的可能, 理想子环 $(a_1, a_2, \dots, a_k)$ 除了 $a_1, a_2, \dots, a_k$ 以外, 还存在着别的个数較小的生成組。例如, 整数环中的理想子环 $(6, 9)$ 不僅由兩個数目 6 和 9 生成, 而且还可以由一个数目 3 生成。

可以由一个数目生成的理想子环叫做 (环 M 中的) 主理想子环, 顯然, 它可以用 (a) 來表示。因此, $(6, 9)$ 就是整数环中的主理想子环 (3) ; 全体偶数就是整数环中的主理想子环 (2) ; 整数环的本身也可以作为一个本身的主理想子环 (1) 來討論; 零理想子环 (0) 不但是整数环的主理想子环, 而且也是任何数环的主理想子环。

§ 3. 整数环中的理想子环、最大公約数

整数整除性的進一步性質密切联系着最大公約数的概念。不过, 我們要預先研究一些整数环中理想子环的性質。

定理 1. 整数环中任何理想子环都是主理想子环。

証明：对于零理想子环，定理是顯然的。因此，我們只討論理想子环 $A \neq (0)$ 。顯然，在不等于零的理想子环 A 的数目中，至少應該存在着一个絕對值最小的数目，我們把它記作 a ，而且把理想子环 A 中的任意数 x 除以 a ： $x = aq + r$ ， $0 \leq r < |a|$ ，其中 q 是商数， r 是余数。因为 x 和 aq 都屬於理想子环 A ，所以它們的差数 $r = x - aq$ 也应该屬於理想子环 A 。由此推出， $r = 0$ ；不然的話， a 就不是那不等于零的理想子环 A 中絕對值最小的一个数目了，也就是：正数 r 小于 $|a|$ 。因此， A 不是別的，就是主理想子环 (a) ，定理被証明了。

除了整数环以外，还存在着別的数字环，它的任何理想子环也都是主理想子环。例如我們可以証明，高斯整数环中的任何理想子环都是主理想子环。

假使数环 M 中的任何理想子环都是主理想子环，那么我們把 M 叫做**主理想子环环**。因此，如果我們不考慮平凡的情况**零环**（即，只由一个数 0 構成的数环）的話，整数环就是第一个主理想子环环的例子。

容易証明，假使 1) M 是非零环，2) M 是主理想子环环，那么 M 應該包含数目 1。

事实上，我們把环 M 的本身当作一个理想子环來研究。这个理想子环應該是主理想子环，所以 $M = (a)$ ，其中 a 是 M 的某一个数，而且，顯然， $a \neq 0$ ，从这里立刻可以推出， M 中的任一数應該有形式 aq ，其中 q 也是 M 中的数目。特別地， $a = aq$ ，因此 $q = 1$ ，即，数目 1 也包含在 M 中。

这样一來，假使一个非零环不包含 1，那么它不可能是一个主理想子环环。另一方面，我們也可以指出一些数环的例子，它們包含了 1，但不是主理想子环环，它們不是在这一方面受到阻碍的。

我們再回到整数环上去，我們把兩個数目 a 和 b 叫做**相伴数**，

如果它們彼此只差一个因子 ± 1 的話。容易証明下面的定理。

定理 2. 整数环中的两个主理想子环 (a) 和 (b) , 当而且只当数目 a 和 b 是相伴数时, 它們是相等(即相合)的。

証明 假設 a 和 b 是相伴数, 而 x 是理想子环 (a) 中的任意数, 根据主理想子环的定义, $x = aq$, 其中 q 是某一整数。因为 a 和 b 是相伴数, 所以 $a = \pm b$. 从这有, $x = bq'$, 其中 $q' = \pm q$, 即, x 不僅属于 (a) , 而且还属于 (b) . 同样地, 假使 x 是理想子环 (b) 中的任意数, 那么 x 也属于 (a) . 因此, $(a) = (b)$.

反过來, 假設 $(a) = (b)$. 于是 $a = bq_1$, $b = aq_2$, 其中 q_1 和 q_2 是整数。換句話說, b/a 及 a/b . 因此, 根据已知的整数整除性質, 我們得到, $a = \pm b$, 即, a 和 b 是相伴数。

現在, 我們要導出最大公約数的概念。

假設 a, b 是任意两个整数, 如果整数 d/a 及 d/b , 那么我們把 d 叫做数目 a 和 b 的公約数。容易看出, 任何一对整数至少具有一个公約数。事实上, 在一切情况中, 数目 1 总是公約数。不过, 除了 1 以外, 还可能存在着别的公約数。例如, 假使 $a=18$, $b=12$, 那么 a 和 b 的公約数有 $d = -1, 1, -2, 2, -3, 3, -6, 6$. 在 a, b 的公約数中, 我們把大于一切其余公約数的公約数叫做最大公約数。例如, 18 和 12 的最大公約数是 6。

假使 $a=0$, $b=0$, 那么任何整数都是 a 和 b 的公約数。因此, 当 a, b 两个数都等于零时, 最大公約数的概念就失掉了意义。以后, 說到最大公約数时, 我們都假定, a 和 b 两个数中至少有一个不等于零。

数目 a 和 b 的最大公約数常用符号 $D(a, b)$ 來表示。例如, $D(18, 12) = 6$ ①

假使两个整数 a, b 的最大公約数等于 1, 那么我們說, 它們是

① 通常用符号 (a, b) (没有字母 D) 來表示数 a, b 的最大公約数, 不过我們不采用这个, 因为这个符号我們是用来表示由 a, b 生成的理想子环的。

互素的。例如, 数目 12 和 25 是互素的, 因为 $\Delta(12, 25) = 1$ 。

类似地, 我們可以引出多个整数最大公約数的概念, 也就是: 有一整数組 $a_1, \dots, a_k (k \geq 2)$, 如果一个整数 d 能够整除每一个 a_i : $d/a_1, \dots, d/a_k$, 那么 d 就叫做整数組 $a_1, \dots, a_k$ 的**公約数**。这个数組的公約数中, 大于其他所有公約数的一个公約数, 叫做这組的**最大公約数**, 我們用符号 $\Delta(a_1, \dots, a_k)$ 来表示数組 $a_1, \dots, a_k$ 的最大公約数。顯然, 当数組中的所有数都等于零时, 最大公約数的概念就失掉了意义。以后, 我們說到最大公約数时, 都假定数組中至少有一个数不等于零。可能会有, 某一整数組的最大公約数等于 1。在这种情况下时, 我們說, 数組是互素的。不过, 不可以推想, 假使数組是互素的, 那么这組的每一对数都是互素的。例如, $\Delta(12, 15, 8) = 1$, 但 $\Delta(12, 15) = 3$ 。

两个或多个数目的最大公約数具有下列基本性質。

1°. 假使 $a_1, \dots, a_k (k \geq 2)$ 是一整数組, 中間至少有一个不等于零, 那么理想子环 $(a_1, \dots, a_k)$ 等于主理想子环 (D) , 其中 D 是数組 $a_1, \dots, a_k$ 的最大公約数, 而且在正整数中, 只有 D 能够生成理想子环 $(a_1, \dots, a_k)$ ①。

証明 理想子环 $(a_1, \dots, a_k)$ 是主理想子环, 因为整数环是主理想子环环, 所以,

$$(a_1, \dots, a_k) = (d), \quad (1)$$

其中 d 是某一整数。顯然, $d \neq 0$, 因为 $(a_1, \dots, a_k) \neq 0$ 。此外 d 可以認為它是正的, 不然的話, 我們可以选取数目 $-d$ 來代替 d , 因为 $(-d) = (d)$ (参考定理 2)。由等式 (1) 可以推出, 数目 $a_1, \dots, a_k$ 應該包含在 (d) 中, 因此 $d/a_1, \dots, d/a_k$, 即 d 是数組 $a_1, \dots, a_k$ 的公約数。現在假設 D 是数組 $a_1, \dots, a_k$ 的最大公約数。于是 $D/a_1, \dots, D/a_k$, 因此 $D/a_1 m + \dots + a_k t$, 其中 $m, \dots, t$ 是任意整数。換句話說, 理想子环 $(a_1, \dots, a_k) = (d)$ 中的任意数 $a_1 m +$

① 在这里以及以下, 所說的都是整数环的理想子环。

$\cdots + a_k t$ 應該包含在理想子環(D)中。特別地, d 應該包含在(D)中, 因此 D/d . 但整數 d 和 D 是正的, 由條件 D/d 的本身可以推出 $D \leq d$. 在另一方面, $D \geq d$, 因為 D 是最大公約數。所以 $d = D$.

2°. 假設 $a_1, \cdots, a_k (k \geq 2)$ 是不同時等於零的整數組。不定方程

$$a_1 x_1 + \cdots + a_k x_k = b, \quad (2)$$

其中 b 是整數, 當而且只當 D/b 時, 其中 D 是組 $a_1, \cdots, a_k$ 的最大公約數, 它關於未知數 $x_1, \cdots, x_k$ 的整數解。

證明 假使方程 (2) 有整數解, 例如 $a_1 m + \cdots + a_k t = b$, 其中 $m, \cdots, t$ 是整數, 那麼 b 包含在理想子環 $(a_1, \cdots, a_k) = (D)$ 中, 而且 D/b . 反過來, 假使 D/b , 那麼 b 包含在理想子環 $(D) = (a_1, \cdots, a_k)$ 中, 因此, 對於某一些整數 $m, \cdots, t$, 我們有 $a_1 m + \cdots + a_k t = b$.

3°. 假使 D 是整數組 $a_1, \cdots, a_k (k \geq 2)$ 的最大公約數, 那麼, 我們可以選取這樣的整數 $\alpha_1, \cdots, \alpha_k$, 使得等式:

$$a_1 \alpha_1 + \cdots + a_k \alpha_k = D$$

成立。

證明 這個性質可以直接由上面的性質推出, 因為這裡的 D 起了 b 的作用。

4°. 整數組 $a_1, \cdots, a_k (k \geq 2)$ 的最大公約數被這組的任一公約數所整除。

證明 假設 D 是組 $a_1, \cdots, a_k$ 的最大公約數, 而 d 是這組的任一公約數。根據性質 3°, $a_1 \alpha_1 + \cdots + a_k \alpha_k = D$, 其中 $\alpha_1, \cdots, \alpha_k$ 是某一些整數。因為 $d/a_1, \cdots, d/a_k$, 所以 $d/a_1 \alpha_1 + \cdots + a_k \alpha_k$. 因此 d/D , 這就是我們所要證明的。

5°. 整數組 $a_1, \cdots, a_k (k \geq 2)$ 當而且只當等式:

$$a_1 \xi_1 + \cdots + a_k \xi_k = 1$$

對於某些整數 $\xi_1, \cdots, \xi_k$ 成立時, 它們是互素的。