# 數論
# 初等教程

A. K. 苏什凱維奇著

高等教育出版社

本書系根据苏联哈尔科夫大学出版社（Издательство харьковского университета）出版的苏什凱維奇（А.К. Сушкевич）著"数論初等教程"（теория чисел - элементарный курс）1954年版譯出。

原書是按对教科書的要求編寫的，可作为綜合大学及师范学院数学系的数論教科書，也可供自修数論的讀者和中学教师参考閱讀之用。

# 数　論

## 初等教程

A.K. 苏什凱維奇著

叶乃聲譯

高等教育出版社出版

北京琉璃廠一七〇号

（北京市書刊出版業營業許可証出字第〇五四号）

京华印書局印刷　新华書店总經售

書号13010·49　開本 850×1168 1/32　印張 8 5/16　字數 198,000

一九五六年九月北京第一版

一九五六年九月北京第一次印刷

印數 0001—5,000　定價（10）¥ 1.30

# 目　錄

# 序

这本数論初等教程是以我的烏克蘭文教科書"数論"(Теорія чисел)的第二版(ДНТВУ, 1936)作为基礎的。前五章基本上保留了烏克蘭版的內容。在第一章中关于素数的各節作了一些擴充；在其余各章中用小号字排印的各節，其內容超出了通常数論初等教程的范圍，統統都取消了。烏克蘭版的第六章("二次形式")整个取消，因为它不在規定的数論課程的正式教学大綱中。另寫了新的兩章來代替它：即第六章——"关于二次形式的若干知識"和第七章——"俄國和苏联数学家在数論方面的成就"。

在國立大学物理数学系和力学数学系所規定的数論教学大綱1952年版(作者：亞·盖尔丰德 А. Гельфонд)中所談到的材料基本上都已包罗在这本教科書里。

这本教科書的对象是大学及师范学院的物理数学系，数学科初学数論的学生，將來的中学数学教师。因此，这教程的講解是初等的，同时列入了大量的数字例題借以闡明所講的理論。除第七章外，在每章末都有習題，其中大部分是計算題。同时注意到那些通常不列入数論教科書、但对中学数学教师來講却是不可缺少的东西，例如十進位循环小数和可約性檢驗法；而且对于連分数的理論也詳加叙述。

第七章是一个概述；僅僅关于切比雪夫的素数个数的估計講得比較詳細。

最后，格·伊·迪潤菲尔德教授惠允審查原稿并提供一系列的宝貴意見，对于这些帮助，我有义务向他表示感謝。

苏什凱維奇教授(Проф. А. Сушкевич)

1953年8月1日于哈尔科夫(Харьков)。

# 第一章　数的可約性

§ 1. 在下文中 $a, b, c, \cdots x, y, \cdots \alpha, \beta, \cdots$ 这些字母我們將只用來表示整数，它可能是正的或負的，已知的或未知的，常数或变数。从初等算術知道，整数的和、差、積仍然是整数，但是兩个整数的商只有在特殊情形下才是整数。对于整数我們來証明下面的基本定理：

**定理 1.** 若 $a$ 及 $b$ 是兩个任意的整数且 $b\neq 0$，那么总可以找到这样的整数 $q$ 及 $r$，使

$$a=bq+r, \tag{1}$$

这兒 $0\leqq r<|b|$①；$r$ 及 $q$ 是唯一确定的。

証　先假設 $a>b>0$。我們來考察数 $b$ 的倍数，即下面的一些数：$1\cdot b=b, 2\cdot b, 3\cdot b, \cdots$，一般地寫作 $k\cdot b$。根据有名的阿基米德公理，对于足够大的 $k$ 有：$k\cdot b>a$。因此，总存在这样一个自然数 $q$，使得恰好有 $bq\leqq a$ 而且 $b(q+1)>a$。我們記：$a-bq=r$；顯然，$r\geqq 0$；由此：$a=bq+r$，而 $b(q+1)=bq+b>a$，

即 $bq+b>bq+r$；由是：$r<b$。对于这个情形定理已被証明。

若 $a=b>0$，則 $q=1, r=0$；若 $b>a>0$，則 $q=0, r=a$，若 $a<0$，$b>0$，則有：$|a|=bq+r$，因此：$a=b(-q)-r$；对于 $r=0$ 公式(1)已成立。对于 $r>0$ 我們記：$b-r=r_1$；$0<r_1<b$；$r=b-r_1$，并得：

$$a=b(-q)-b+r_1=b(-q-1)+r_1;$$

因为 $0<r_1<b$，所以这是与公式(1)相同的式子。

---

① 通常我們用 $|x|$ 表示数 $x$ 的絕对值，也就是当 $x>0$ 时，$|x|=x$；当 $x<0$ 时，$|x|=-x$；而 $|0|=0$。

最后，对于 $b<0$ 根据已經証明的我們有：

$$a=|b|q+r; \qquad 0\leqq r<|b|;$$

因此：

$$a=b(-q)+r,$$

即是仍然得到公式(1)。

現在証明 $q$ 及 $r$ 是唯一确定的。

假定我們由兩个方法得到：

$$a=bq+r=bq_1+r_1, \quad \text{这兒 } 0\leqq r<|b|, \quad 0\leqq r_1<|b|,$$

于是：

$$bq-bq_1=r_1-r; \quad b(q-q_1)=r_1-r.$$

在这里等式右边絕对值小于 $|b|$，但是左边能被 $b$ 除尽；因此，$r_1-r=0$, $r_1=r$, $q_1=q$；于是定理 1 已經完全被証明了。

注意　对于所給(正)的 $a$ 和 $b$，数 $q$ 及 $r$ 的求法乃是自然数的通常的"帶余数除法"，它在初等算術中已講过了。在这里我們嚴格地証明了：对于任意整数 $a$ 及 $b$，数 $q$ 及 $r$ 是存在的；$q$ 是以 $b$ 除 $a$ 所得的不完全商数，$r$ 是所得的余数。

以 $b$ 除等式(1)的兩边，我們得到：

$$\frac{a}{b}=q+\frac{r}{b}. \tag{2}$$

在这里左边(当 $|a|\geqq b>0$ 时)是假分数，但是 $\frac{r}{b}$ 总是眞分数；公式(2)表示从假分数中分出整数部分；$q$ 是分数 $\frac{a}{b}$ 的整数部分；記为：

$$q=\left[\frac{a}{b}\right]=E\left(\frac{a}{b}\right).$$

注意　在一般情形，若 $x$ 是任意实数(有理数或無理数，正数或負数)，則称適合 $[x]\leqq x<[x]+1$ 的整数 $[x]$ 或 $E(x)$ 为其整数部分，当 $x$ 是整数时 $[x]=x$。

相仿地就引用記号：$\{x\}=x-[x]$；$\{x\}$ 是数 $x$ 的分数部分；$\{x\}$ 总是非負的。最后，用 $(x)$ 表示数 $x$ 到与 $x$ 最近的整数的距离，

即是 $x$ 和与 $x$ 最近的整数之差的絕对值，也就是二数 $\{x\}$ 及 $1-\{x\}$ 中的最小的。

当 $r=0$ 时的情形是值得注意的；这时公式(1)变成 $a=bq$，或 $\frac{a}{b}=q$。在这个情形就說：$a$ 被 $b$ 除尽(即除尽無余)，$b$ 是数 $a$ 的約数或因数；$a$ 是数 $b$ 的倍数。

§ 2. **定理 2.** 若 $a$ 被 $b$ 除尽，而 $b$ 被 $c$ 除尽，則 $a$ 也被 $c$ 除尽。

**証** 这可由乘法的結合律導出：我們有：$a=bq$, $b=cq_1$, 因此：

$$a=(cq_1)q=c(qq_1).$$

**定理 2** 表示所謂可約性的"傳遞律"。

**定理 3.** 若 $a_1, a_2, \cdots a_k$ 都被 $c$ 除尽，而 $x_1, x_2, \cdots x_k$ 是任意的(整)数，則 $a_1x_1+a_2x_2+\cdots+a_kx_k$ 也被 $c$ 除尽。

**証** 这可由分配律導出：

$$a_1=cb_1,\quad a_2=cb_2,\ \cdots a_k=cb_k;$$

由此：

$$a_1x_1+a_2x_2+\cdots+a_kx_k=c(b_1x_1+b_2x_2+\cdots+b_kx_k).$$

**定理 4.** 若 $a$ 被 $b$ 除尽，則一般 $\pm a$ 被 $\pm b$ 除尽，特别 $|a|$ 被 $|b|$ 除尽。

**証** $a=bq=(-b)(-q)$； $-a=b(-q)=(-b)q$.

**定理 5.** 每一个数自己被自己除尽。

**証** $a=a\cdot 1$。

**定理 6.** $\pm 1$ 是任何数的約数，除了 $\pm 1$ 沒有别的数有这样的性質。

**証** $a=1\cdot a=(-1)(-a)$。若 $a$ 是任何数的約数，則 1 也被 $a$ 除尽；但是 1 只能被 $\pm 1$ 除尽。

**定理 7.** 0 被任何数除尽；除零而外沒有别的数具有这样的性質。

証 $0=a\cdot 0$；若 $a\neq 0$，則 $a$ 不可能被 $a+1$ 除尽。

定理 4 使其在可約性問題中可以只限于正数。因此在本章中我們所用的文字不但僅表示整数，而且僅僅表示正整数。譬如說，談到数的可約性时，我們所注意的是它的正約数。一般說來，在可約性問題中，数 $a$ 及 $-a$ 的作用相同；这样的数（相差一个符号或相差一个因数 $-1$）称为相联数。

§ 3. **最小公倍数** 設 $a_1, a_2, \cdots a_n$ 是所給的（正整）数；它們的乘積 $a_1a_2\cdots a_n$ 能被它們当中每一个所除尽，也就是它們的公倍数。这样的公倍数有無数多个，因为对于任意的整数 $k$ 來說，$ka_1a_2\cdots a_n$ 也是所給諸数的公倍数；数 0 也是它們的公倍数。因此，存在一个这些数的最小的正的倍数。这就是所謂的最小公倍数。我們用 $m$ 來表示它。

或用記号：$m=M(a_1, a_2, \cdots a_n)=\{a_1, a_2, \cdots a_n\}$。

顯然，$0<m\leqq a_1a_2\cdots a_n$。

設 $m_1$ 是同样这些数 $a_1, a_2, \cdots a_n$ 的任一別的公倍数；則我們以 $m$ 除 $m_1$ 并由定理 1 得到：

$$m_1=mq+r;\quad 0\leqq r<m.$$

由是 $r=m_1-mq$，按照定理 3 我們導出：$r$ 也是这些数 $a_1, a_2, \cdots a_n$ 的公倍数。但是 $r<m$，而 $m$ 是最小公倍数；所以 $r=0$，从而我們得到：

**定理 8.** 在若干个所給数的所有公倍数当中，总可找到这样的一个公倍数，它是这些数的任何別的公倍数的約数；这就是最小公倍数。

§ 4. **最大公約数** 任意 $n$ 个（正整）数总是有一个等于 1 的公約数。如果除 1 外（更好是說成除了 $\pm 1$ 而外）它們沒有別的公約数，則这样的諸数称为是互素的。但是除 1 外，所給諸数还可以有別的公約数，这一事实是可能發生的（例如，若它們全是偶数，則

2 也是它們的公約数)。不論在怎样的情形下，所給一些数的公約数的个数总是有限的，因为它們中的每一个(按絕对值)都不可能大于所給諸数中的最小的。設 $d', d'', d''', \cdots$ 是所給諸数的所有(正)公約数而

$$d = M(d', d'', d''', \cdots).$$

所給諸数 $a_1, a_2, \cdots a_n$ 中的每一个都是所有約数 $d', d'', d''', \cdots$ 的公倍数，因而(按定理 8)也都能被 $d$ 除尽。可見 $d$ 也是所給諸数的公約数，也就是 $d$ 包含在諸数 $d', d'', d''', \cdots$ 的集合之中。同时，$d$ 顯然是所有这些約数中的最大者，因为 $d$ 能被它們中的每一个所除尽。我們用記号：

$$d = D(a_1, a_2, \cdots a_n) = (a_1, a_2, \cdots a_n).$$

因而有：

**定理 9.** 在所給諸数的所有公約数中存在着这样一个公約数：它能被这些数的任何别的公約数所除尽；这就是所給諸数的最大公約数。

**定理 10.** 当而且僅当商数 $\frac{a_1}{d}, \frac{a_2}{d}, \cdots \frac{a_n}{d}$ 互素时，数 $d$ 才是諸数 $a_1, a_2, \cdots a_n$ 的最大公約数。

証 1. 設 $d = D(a_1, a_2, \cdots a_n)$，并設商数 $\frac{a_1}{d}, \frac{a_2}{d}, \cdots \frac{a_n}{d}$ 有公約数 $\delta > 1$。則商数 $\frac{a_1}{d\delta}, \frac{a_2}{d\delta}, \cdots \frac{a_n}{d\delta}$ 都是整数，即是 $a_1, a_2, \cdots a_n$ 有公約数 $d\delta > d$，但这是与 $d$ 为最大公約数相矛盾的。

2. 現在設諸数 $\frac{a_1}{d}, \frac{a_2}{d}, \cdots \frac{a_n}{d}$ 互素；設 $d$ 不是最大公約数；則按定理 9，$D(a_1, a_2, \cdots a_n)$ 有形式：$d\delta$，这兒 $\delta > 1$。从而 $\frac{a_1}{d\delta} = \frac{a_1}{d} : \delta$，$\frac{a_2}{d\delta} = \frac{a_2}{d} : \delta, \cdots \frac{a_n}{d\delta} = \frac{a_n}{d} : \delta$ 都是整数，即 $\delta > 1$ 是諸数 $\frac{a_1}{d}, \frac{a_2}{d}, \cdots \frac{a_n}{d}$ 的公約数，这是与这些数互素相矛盾的。

**定理 11.** 若 $d = D(a_1, a_2, \cdots a_n)$，則 $D(a_1k, a_2k, \cdots a_nk) = dk$，

$D\left(\frac{a_1}{k}, \frac{a_2}{k}, \cdots \frac{a_n}{k}\right)=\frac{d}{k}$（只有在 $k$ 是諸数 $a_1, a_2, \cdots a_n$ 的一个公約数时，后式才成立）。

証 这个定理可由 $\frac{a_\lambda}{d}=\frac{a_\lambda k}{dk}=\frac{a_\lambda : k}{d : k}$ 根据定理 10 得到。

§ 5. 我們來研究所給的是兩个数 $a$ 及 $b$ 的情形。設 $m=M(a, b)$；按定理 8，$ab$ 能被 $m$ 除尽。我們記：

$$\frac{ab}{m}=d;$$

于是：

$$\frac{a}{d}=\frac{m}{b};\quad \frac{b}{d}=\frac{m}{a}.$$

右边是整数，从而左边也是整数，因此 $d$ 是二数 $a$ 及 $b$ 的公約数。設 $d'$ 是它們的另外任一公約数，則：

$$\frac{ab}{d'}=a\cdot\frac{b}{d'}=b\cdot\frac{a}{d'},$$

即 $m'=\frac{ab}{d'}$ 是二数 $a$ 及 $b$ 的公倍数。按定理 8，$m'$ 应被 $m$ 除尽：

$$\frac{m'}{m}=\frac{ab}{d'}:\frac{ab}{d}=\frac{d}{d'}.$$

因为这是整数，即 $d$ 能被 $d'$ 除尽，所以（参閱定理 9）$d$ 是二数 $a$ 及 $b$ 的最大公約数。

因而有：

**定理 12.** 若 $m=M(a, b), d=D(a, b)$，則

$$ab=md. \tag{3}$$

当 $d=1$ 时从(3)直接導出：

推論 当而且僅当二数 $a$ 及 $b$ 的最小公倍数等于它們的乘積时，二数 $a$ 及 $b$ 互素。

注意若所給的数多于兩个，則这推論并不眞实：互素的几个数其最小公倍数也可能不等于它們的乘積。例如：

$$D(6, 4, 9)=1,\ \text{但是}\ M(6, 4, 9)=36<6\cdot4\cdot9.$$

在下文中我們还要回到这个問題上来（参閱定理 17）。

§ 6. **定理 13.** 为了求几个数的最大公約数，可以先求其中任何二数的最大公約数，然后求这个所得的数与所給数中任何第三数的最大公約数，其次再求第二次所得的数与所給数中任何第四数的最大公約数，以下类推。这样下去最后所得的公約数也就是全部所給数的最大公約数。

証　只要对于三个所給数 $a, b, c$ 来証明这个定理就够了。对于許多个所給数，这个定理的証明是相仿的。因此，設 $D(a, b)=e$, $D(e, c)=d$；按定理 2, $a$ 及 $b$ 都能被 $d$ 除尽，即 $d$ 是 $a, b, c$ 的公約数。設 $d'$ 是 $a, b, c$ 的任何别的公約数；則(按定理 9) $e$ 能被 $d'$ 除尽，从而(按同样的定理 9), $d$ 也能被 $d'$ 除尽，即 $d$ 是 $a, b, c$ 的最大公約数。公式的形式为

$$D(a, b, c)=D(D(a, b), c).$$

对于最小公倍数也有相仿的定理。

**定理 14.** 为了求几个数的最小公倍数，可以先求其中任何二数的最小公倍数，然后求这个所得的数与所給数中第三数的最小公倍数，以下类推。最后所得的公倍数也就是全部所給数的最小公倍数。

这个定理也是只要对于三个所給数 $a, b, c$ 来証明就够了。証明完全和定理 13 的証明相仿(不过不用定理 9 而应該引用定理 8 罢了)，我們把它留給讀者去做。

也可以用公式來表示这个定理：

$$M(a, b, c)=M(M(a, b), c).$$

这样一来，求几个数的最大公約数(或最小公倍数)的問題便化成了求僅僅兩个数的最大公約数(或最小公倍数)問題。至于求兩个数的最大公約数的具体方法我們在下一章中就要講到。

§ 7. **定理 15.** 若 $ab$ 能被 $c$ 除尽，而 $a$ 与 $c$ 互素，則 $b$ 必能被 $c$ 除尽。

証 $ab$ 既能被 $a$ 除尽又能被 $c$ 除尽，因而(按定理 8)，也能被它們的最小公倍数除尽，按定理 12 的推論，这个最小公倍数等于它們的乘積：$M(a,c)=ac$；因此，$\frac{ab}{ac}=\frac{b}{c}$ 是一个整数。

定理 16. 若 $a$ 与 $c$ 互素，則：

$$D(ab,c)=D(b,c).$$

証 設 $D(b,c)=d$；則 $ab$ 也能被 $d$ 除尽。反之，設 $D(ab,c)=d$；則 $D(a,d)=1$，因为否則(按定理 2) $a$ 与 $c$ 就不可能是互素的。因此：$ab$ 能被 $d$ 除尽，而 $a$ 与 $d$ 互素；由定理 15，在这情形下 $b$ 也能被 $d$ 除尽。定理也就被証明了。

注意定理 15 乃是定理 16 当 $d=c$ 时的特殊情形。

如果不僅 $D(a,c)=1$，而且 $D(b,c)=1$，則由定理 16：

$$D(ab,c)=1.$$

意卽：

推論 1. 若 $c$ 与 $a$ 互素，$c$ 与 $b$ 也互素，則 $c$ 与乘積 $ab$ 也互素。

这个推論可直接擴張到几个因数的情形。

推論 2. 若諸数 $a_1, a_2, \cdots a_m$ 中每一个与諸数 $b_1, b_2, \cdots b_n$ 中每一个互素，則乘積 $a_1a_2\cdots a_m$ 与 $b_1b_2\cdots b_n$ 也互素。

若 $a_1=a_2=\cdots=a_m$ 且 $b_1=b_2=\cdots=b_n$，則得：

推論 3. 若 $a$ 与 $b$ 互素，則 $a$ 的任何乘冪也与 $b$ 的任何乘冪互素①。

§ 8. 我們現在來研究，在怎样的情形下几个数的最小公倍数等于它們的乘積。設所給的是三个数 $a, b, c$。按定理 14，为了去求 $M(a,b,c)$，我們先求 $M(a,b)$；若 $M(a,b)<ab$，則 $M(a,b,c)<abc$。因此，应該有 $M(a,b)=ab$，故而(按定理 12 的推論) $D(a,b)=1$。

① 当然，这里所指的是所有这些乘冪的方次数都是正整数。

其次，我們有：$M(a,b,c)=M(ab,c)$；要这式等于 $abc$，就应該有 $D(ab,c)=1$，从而顯然，$D(a,c)=1, D(b,c)=1$。这样一來，三数 $a,b,c$ 中每兩个是互素的，換句話說，三数 $a,b,c$“兩兩互素”。

反之，現在如果已知三数 $a,b,c$ 兩兩互素；在这个情形下 $M(a,b)=ab$。由定理 16 的推論 1，則 $ab$ 与 $c$ 也互素，即：$M(a,b,c)=M(ab,c)=abc$。

这也可以直接擴張到几个数的情形。

因而有：

**定理 17.** 当而且僅当几个数兩兩互素时，它們的最小公倍数才等于它們的乘積。

推論　若数 $c$ 能被諸数 $a_1, a_2, \cdots a_n$ 中每一个所除尽，而这几个数兩兩互素，則 $c$ 也能被乘積 $a_1a_2\cdots a_n$ 所除尽。

这可由定理 17 及定理 8 直接導出。

§ 9. **某些应用**　1. 設 $x$ 是整数；我們証明：若 $\sqrt[n]{x}$ 不是整数，則这个根数不可能是有理数。假定 $\sqrt[n]{x}=\frac{a}{b}$，这兒 $\frac{a}{b}$ 是不可約分数，即 $D(a,b)=1$。則 $x=\frac{a^n}{b^n}$，并且按定理 16 的推論 3，分数 $\frac{a^n}{b^n}$ 也是不可約分数，因而当 $b>1$ 时不可能等于整数 $x$。

一般言之，具有整系数而且最高次項的系数等于一的 $n$ 次代数方程不可能有有理分数根。

設这样的方程是：

$$x^n+a_1x^{n-1}+a_2x^{n-2}+\cdots+a_n=0 \qquad (4)$$

并且 $x=\frac{a}{b}$ 是它的有理根，同时 $D(a,b)=1$。將这个 $x$ 値代入方程(4)并以 $b^{n-1}$ 乘兩边，我們得到：

$$\frac{a^n}{b}+a_1a^{n-1}+a_2ba^{n-2}+\cdots+a_nb^{n-1}=0.$$

在这里当 $b>1$ 时第一項是分数(仍按定理 16 的推論 3)，但是所有其余各項都是整数；如此相加决不可能等于零。因此，必然

要 $b=1$, 即 $x=a$ 是整根。

注意(4)型的方程之根若非有理数，則称之为代数整数。

2. 我們討論二項系数：

$$\binom{b}{a}=\frac{b(b-1)(b-2)\cdots(b-a+1)}{1\cdot 2\cdot 3\cdots a}$$

其中 $b\geqq a$。我們有：

$$\binom{b}{b}=1,\quad \binom{b}{1}=b;$$

另外有記号：

$$\binom{b}{0}=1,\quad \text{当 } a>b \text{ 时 } \binom{b}{a}=0.$$

由直接計算容易導出公式：

$$\binom{b}{a}=\binom{b-1}{a}+\binom{b-1}{a-1}. \tag{5}$$

由此我們用完全归納法導出：$\binom{b}{a}$总是整数。其次，有：

$$\binom{b}{a}=\frac{b}{a}\binom{b-1}{a-1}. \tag{6}$$

設 $b>a$ 且 $D(a,b)=1$。由公式(6)得知：$b\cdot\binom{b-1}{a-1}$能被 $a$ 除尽，从而，按定理 15, $\binom{b-1}{a-1}$ 能被 $a$ 除尽。故而由公式(6)推知：$\binom{b}{a}$能被 $b$ 除尽。

因此，当 $a$ 与 $b$ 互素时$\binom{b}{a}$能被 $b$ 除尽。

§ 10. **素数** 在所有的整数中間，数 $\pm1$ 及 0 与众不同；$\pm1$ 只有一个約数 1[①]；0 能被任何整数除尽，即有無数多个約数。此外任何整数 $a$ 至少有兩个約数：1 及 $|a|$；如果它除这兩个約数外再沒有别的任何(整)約数的話，那么就称它为素数；否則称它为合成数。

① 我們所考慮的只是正的約数。