内 容 简 介

本书内容包括数的整除性，同余式，二次剩余，原根和指数，不定方程，数论函数等六章，介绍了初等数论中的基本的知识、概念和方法，并为今后学习近世代数提供了一些数论方面的具体素材、实例以及数学修养方面的知识。书中配有一定量的习题，书末附有解答提示。

本书可供高等院校数学各专业使用。

初 等 数 论

冯克勤 余红兵 编

责任编辑：刘卫东 封面设计：王瑞荣

*

中国科学技术大学出版社出版

（安徽省合肥市金寨路96号）

合肥炮兵学院教学印刷厂印刷

新华书店总店科技发行所发行

*

开本：850×1168/32 印张：5.5 字数：141千

1989年12月第1版 1989年12月第1次印刷

印数：3000册

ISBN-7-312-00135-5/O·59 定价：1.40元

前　言

初等数论是研究整数性质和方程（组）整数解的一门数学学科。这是一门古老的数学分支。早在公元前三世纪，古希腊数学家欧几里德（Euclid）证明了素数有无穷多个，并且给出了求两个正整数最大公因子的辗转相除法。我国古代的《孙子算经》中给出解一次同余方程组的方法，即著名的孙子定理，国外把它叫作中国剩余定理。从十七世纪到十九世纪，费马（Fermat），欧拉（Euler），勒让德（Legendre），高斯（Gauss）等人的工作大大丰富和发展了初等数论的内容。

初等数论中有许多问题是一般人都可以听懂的。但是有些问题非常难解，甚至经过不少大数学家长时间的努力都未能解决，而这些数论问题也因此更加著名。当然，几个世纪过程中数学家在初等数论中的努力不是徒劳的，他们在解决或致力于解决初等数论问题的过程中，引入了许多新的思想，创造了新的方法和概念，推动了数学（特别是数论和代数学）的发展。这些新思想，新方法和新概念的提出和完善，往往比解决某个具体数论问题具有更重要的意义。

初等数论不仅是“思维的体操”和数学游戏，在当前计算机时代和信息社会，初等数论和其他离散数学分支（如组合数学，图论，近世代数等）一样，在计算机科学、通信工程、离散控制系统、代数编码等许多领域得到日益广泛的实际应用。初等数论不仅是数学工作者，而且也是许多从事应用和实际工作的工程技术人员所不可缺少的数学知识。

中国科学技术大学从一九七七年起就在大学一年级开设初等

数论必修课。十年来经过许多教师的讲授，积累了不少经验，本讲义是在大家的讲义和丰富经验的基础上写成的，是一本为大学一年级一学期约四十学时（每周二学时）用的教材。这本讲义的目的主要有两个：一个是介绍初等数论中最基本的知识、概念和方法。另一个则是为今后学习近世代数提供一些数论方面的具体素材、实例以及数学修养方面的知识。

本书配有一定量的习题，书末还附有这些习题的解答提示。这些解法未必是最好的，只供参考。

编　者

1988年10月于合肥

目　　录

第一章　数的整除性

§1　数的整除性

初等数论的基本研究对象是整数集合

$$Z=\{0,\ \pm1,\ \pm2,\ \pm3,\ \cdots\}$$

和自然数集合（即正整数集合）

$$N=\{1,\ 2,\ 3,\ 4,\ \cdots\}。$$

在集合N中可以进行加法和乘法运算，即两个自然数之和或乘积仍旧是自然数。在集合Z中除了加法和乘法之外还可作减法运算，并且这些运算满足一些规律（即：加法和乘法的结合律和交换律，加法与乘法的分配律），但是一般不能作除法，也就是说，设a和b是整数，$b\neq0$，则a/b不一定是整数。即不一定存在整数c，使得$a=bc$。由此产生出初等数论中第一个基本概念：数的整除性。

定义　设a和b是整数，$b\neq0$，如果存在整数c使得$a=bc$，则称为b**整除**a，表示成$b\mid a$，并且称b是a的一个因子，而a为b的倍数。如果不存在整数c使得$a=bc$，则称b**不整除**a，表示成$b\nmid a$。

例如：$(-3)\mid 6$，$3\mid(-6)$，$4\nmid 6$。对每个整数n，$(\pm1)\mid n$。对每个非零整数n，$n\mid 0$，$n\mid(\pm n)$。

由整除的定义不难看出，数的整除性有如下一些基本性质。

(1) 设a，$b\in Z$，$b\neq0$。如果$a\mid b$，则$|a|\leqslant|b|$。从而每个非零整数的因子只有有限多个。

这是因为：若 $a \mid b$，则有 $c \in Z$，使得 $b=ac$。从而 $|b|=|a| \cdot |c|$，并且 $|c| \in Z$，所以 $|a| \mid |b|$。因为 $b \neq 0$，从而 $c \neq 0$，即 $|c| \geqslant 1$。于是 $|b|=|a| \cdot |c| \geqslant |a|$。这表明 b 的每个因子的绝对值均不超过 b 的绝对值，从而 b 只有有限多个因子。

(2) 若 $a \mid b$，$c \in Z$，则 $a \mid bc$。

(3) 若 a，$b \in Z$，$a \neq 0$，$b \neq 0$。如果 $a \mid b$，$b \mid a$，则 $a=\pm b$。

这是因为：由性质(1)知道 $a \mid b \Longrightarrow |a| \leqslant |b|$，而 $b \mid a \Longrightarrow |b| \leqslant |a|$。因此若 $a \mid b$，$b \mid a$，则 $|a|=|b|$，即 $a=\pm b$。

(4) 若 $a \mid b$，$b \mid c$，则 $a \mid c$。

(5) 若 $a \mid b$，$a \mid c$，t，$s \in Z$，则 $a \mid bt+cs$。

这是因为：由 $a \mid b$ 和 $a \mid c$ 可知存在 $x, y \in Z$，使得 $b=ax$，$c=ay$。于是 $bt+cs=a(xt+ys)$。由于 $xt+ys \in Z$，从而 $a \mid (bt+cs)$。

定义 设 α 为任意实数，我们以 $[\alpha]$ 表示不超过 α 的最大整数，叫作 α 的**整数部分**。而 $\alpha-[\alpha]$ 叫作实数 α 的**分数部分**，表示成 $\{\alpha\}$。

于是 $\alpha=[\alpha]+\{\alpha\}$，$[\alpha] \in Z$，$0 \leqslant \{\alpha\} < 1$。并且 $\alpha \in Z \Longleftrightarrow \alpha=[\alpha] \Longleftrightarrow \{\alpha\}=0$。例如，$[2.1]=2$，$\{2.1\}=0.1$。$[\pi]=3$，$\{\pi\}=\pi-3$。$[-0.1]=-1$，$\{-0.1\}=0.9$。

现在我们给出整数的一个基本性质。

定理 1（带余除法） 设 a，$b \in Z$，$b>0$，则存在唯一决定的整数 q 和 r，使得

$$a=qb+r, \quad 0 \leqslant r < b。$$

证明 先证满足条件的 q 和 r 是存在的，为此令 $q=\left[\frac{a}{b}\right]$，$r=a-qb$，则 q 和 r 均是整数，并且由于 $\frac{r}{b}=\frac{a}{b}-q=\left\{\frac{a}{b}\right\}$，

而$0\leqslant\left\{\frac{a}{b}\right\}<1$，从而$0\leqslant\frac{r}{b}<1$，即$0\leqslant r<b$。

再证q和r是唯一决定的。如果又有整数q'和r'使得$a=q'b+r', 0\leqslant r'<b$,则$|r-r'|<b$，并且$r-r'=b(q'-q)$。这表明$r-r'$是正整数$b$的倍数，并且$r-r'$的绝对值又小于$b$。这只可能$r=r'$，从而$q=q'$。证毕。

定义 设a和b是不全为零的整数，a和b的**最大公因子**是指满足下述二条件的整数d：

(1) d为a和b的公因子，即$d\mid a$并且$d\mid b$。

(2) d为a和b的所有公因子中最大的，即对整数c，如果$c\mid a$并且$c\mid b$，则$c\leqslant d$。

我们知道，每个非零整数只有有限多个因子，所以若a和b是整数并且不全为零，那末它们的公因子也只有有限多个。所以它们的最大公因子必然存在并且是唯一的。今后把a和b的最大公因子表示成(a, b)，注意若n是a和b的公因子，则$-n$也是它们的公因子。所以最大公因子一定是正整数。

类似地，对于不全为零的任意有限个整数$a_1, a_2, \cdots, a_n$我们也可定义它们的最大公因子，表示成$(a_1, a_2, \cdots, a_n)$。

例如，$(4,-6)=2$，$(0, 6)=6$，$(6, 15, -18)=3$。

如果$a, b\in Z$，$(a, b)=1$，则称a和b是**互素**的。换句话说，整数a和b是互素的，即指它们只有公因子±1。例如4和-15是互素的。

类似地可以定义最小公倍数。

定义 设a和b是两个非零整数，整数D叫作a和b的**最小公倍数**，是指D满足以下两个条件：

(1) D为正整数，并且D是a和b的公倍数。即$D\geqslant1$并且$a\mid D$，$b\mid D$。

(2) D是a和b的最小的正公倍数。即若又有$D'\geqslant1$，

$a \mid D'$，$b \mid D'$，则$D \leqslant D'$。

任意两个非零整数a和b均存在正公倍数$|ab|$，从而也必然存在最小的正公倍数D。我们今后把a和b的最小公倍数表示成$[a, b]$，对于任意有限个非零整数a_1，a_2，…，a_n，我们也可定义它们的最小公倍数$[a_1, a_2, \cdots, a_n]$。

由定义可以证明：设a，b，c是非零整数，则

$(a, b, c)=((a, b), c)$，$[a, b, c]=[[a, b], c]$。

我们说过，初等数论的主要课题是研究整数的性质和方程（组）的整数解，现在我们可以求一些简单方程的整数解问题。最简单的方程当然是一元一次方程

$$ax=b,$$

其中a和b均是整数，并且$a \neq 0$。根据整除性的定义，这个方程有整数解x的充分必要条件是$a \mid b$，并且当$a \mid b$时，方程有唯一的整数解$x=\dfrac{b}{a}$。除了这个方程之外，另一类简单的方程是二元一次方程

$$ax+by=c, \tag{1}$$

其中a，b，$c \in Z$，并且a和b不全为零。我们要问：方程(1)何时有整数解(x, y)？

我们用下述方式来研究方程(1)的整解问题：给了整数a和b（不全为零），考查集合

$$S=\{ax+by \mid x, y \in Z\}。$$

于是方程（1）有整数解的充要条件是$c \in S$。所以，若集合S清楚了，就可判别方程（1）是否有解。现在我们可以完全地刻划集合S。

引理1 （1）若$m, n \in S$，则$m \pm n \in S$。

（2）若$n \in S$，$c \in Z$，则$cn \in S$。

（3）设d为集合S中的最小正整数，则S恰好是d的所有倍数构成的集合。

(4) $d=(a, b)$。

证明 (1) 若 m 和 $n \in S$，则有整数 x_1，x_2，y_1，y_2 使得 $m=ax_1+by_1$，$n=ax_2+by_2$，于是 $m \pm n=a(x_1 \pm x_2)+b(y_1 \pm y_2)$，从而 $m \pm n \in S$。类似可证(2)。

(3) 由于 a 和 b 不全为零，并且 $|a|, |b| \in S$，可知 S 中包含正整数，设 d 是 S 中最小的正整数。对于每个 $c \in S$。由带余除法可知存在 q 和 $r \in Z$，使得 $c=qd+r$，$0 \leqslant r < d$。由于 c，$d \in S$，利用前面(1)和(2)可知 $r=c-qd \in S$，但是 d 为 S 中最小的正整数，而 $0 \leqslant r < d$，从而 $r=0$。于是 $c=qd$，即 c 为 d 的倍数。反过来，由(2)可知 d 的倍数均属于 S。因此 S 就是 d 的所有倍数构成的集合。

(4) 设 $D=(a, b)$，我们来证 $D=d$。由于 $d \in S$，从而存在 x，$y \in Z$，使得 $d=ax+by$，因为 $D \mid a$，$D \mid b$，因此 $D \mid ax+by=d$，特别地 $D \leqslant d$。另一方面，因为 $a=a \cdot 1+b \cdot 0 \in S$，从而由(3)知 a 是 d 的倍数。同样地，b 也是 d 的倍数。所以 d 是 a 和 b 的公因子，于是 $d \leqslant D$。这就表明 $d=D$。证毕。

引理1表明，集合 S 恰好是由 (a, b) 的所有倍数构成的。换句话说，我们证明了

系 设 a 和 b 是不全为零的整数，c 为整数，则方程 $ax+by=c$ 有整数解的充分必要条件是 $(a, b) \mid c$。特别地：(1)存在整数 x 和 y，使得 $ax+by=(a, b)$；(2) a 和 b 互素，则存在整数 x 和 y，使得 $ax+by=1$。

利用引理1我们可以得到最大公因子的一些有用的性质。

引理2 (1) 设 m 为正整数，则 $(ma, mb)=m(a, b)$。

(2) 若 $(a, b)=d$，则 $\frac{a}{d}$ 和 $\frac{b}{d}$ 是互素的整数。

(3) a 和 b 的每个公因子都是 (a, b) 的因子。

(4) 若 $(a, m)=(b, m)=1$，则 $(ab, m)=1$。

(5) 若 a 和 b 是不全为零的整数，则对每个整数 x 有

$$(a,\ b)=(a,\ b+ax)。$$

(6) 若 $c \mid ab$，$(c,\ b)=1$，则 $c \mid a$。

证明 (1) $(ma,\ mb)=$ 形如 $max+mby$ 的最小正整数 $=m\cdot$形如 $ax+by$ 的最小正整数$=m(a,\ b)$。

(2) 显然 $\frac{a}{d}$，$\frac{b}{d}\in Z$，并且 $d=(a,b)=(d\cdot\frac{a}{d},d\cdot\frac{b}{d})$

$=d(\frac{a}{d},\ \frac{b}{d})$，因此$(\frac{a}{d},\ \frac{b}{d})=1$。

(3) 设 m 为 a 和 b 的公因子。则 $a=ma'$，$b=mb'$，a'，$b'\in Z$。于是$(a,\ b)=(ma',\ mb')=m(a',\ b')$，所以 $m \mid (a,\ b)$。

(4) 由于$(a,\ m)=1$，从而有 $x,\ y\in Z$ 使得 $ax+my=1$。同样由$(b,\ m)=1$ 可知有 $x',y'\in Z$，使得 $bx'+my'=1$。将两式相乘可知

$$ab(xx')+m(axy'+bx'y+myy')=1,$$

这就表明$(ab,\ m)=1$。

(5) 设 $g=(a,\ b)$，$h=(a,\ b+ax)$。由于 $g \mid a$，$g \mid b$，从而 $g \mid b+ax$。即 g 是 a 和 $b+ax$ 的公因子，于是 $g\leqslant h$。另一方面，$h \mid a$，$h \mid (b+ax)$，从而 $h \mid (b+ax)-ax=b$。即 h 是 a 和 b 的公因子，于是 $h\leqslant g$，因此 $h=g$。

(6) 已知 $c \mid ab$，又显然有 $c \mid ac$。从而由(3)可知 $c \mid (ab,\ ac)$。但是$(ab,\ ac)=a(b,\ c)=a$，于是 $c \mid a$。证毕。

利用引理2，我们可以得到求最大公因子$(a,\ b)$的如下算法：（由于$(a,\ b)=(|a|,\ |b|)$，不妨设 $a\geqslant b>0$。）

欧几里德算法 设 $a,\ b\in Z$，$a\geqslant b>0$。按下述方式反复作带余除法（有限步后必可除尽）。

用 b 除 a：$a=bq_0+r_0$，$0<r_0<b$。

用 r_0 除 b：$b=r_0q_1+r_1$，$0<r_1<r_0$。

用 r_1 除 r_0：$r_0=r_1q_2+r_2$，$0<r_2<r_1$。

……

用 r_{n-1} 除 r_{n-2}：$r_{n-2}=r_{n-1}q_n+r_n$，$0<r_n<r_{n-1}$。

用 r_n 除 r_{n-1}：$r_{n-1}=r_nq_{n+1}$。

则 $$(a, b)=r_n。$$

证明 由于 $b>r_0>r_1>\cdots>r_{n-1}>\cdots>0$，从而上面带余除法有限步必然除尽。并且由引理2的（5）可知 $(a, b)=(b, a-bq_0)=(b, r_0)=(r_0, r_1)=\cdots=(r_{n-1}, r_n)=r_n$。证毕。

注记 上面的算法不仅可用来求 (a, b)，而且还可以具体求出方程 $ax+by=(a, b)$ 的一组整解。让我们以例说明。

例 设 $a=963$，$b=657$。上述欧氏算法为

$$963=1\cdot 657+306,$$

$$657=2\cdot 306+45,$$

$$306=6\cdot 45+36,$$

$$45=1\cdot 36+9,$$

$$36=4\cdot 9。$$

于是 $(963, 657)=9$。并且

$$9=45-1\cdot 36=45-(306-6\cdot 45)=7\cdot 45-306$$

$$=7(657-2\cdot 306)-306=7\cdot 657-15\cdot 306$$

$$=7\cdot 657-15(936-657)=22\cdot 657-15\cdot 936。$$

从而 $x=-15$，$y=22$ 就是方程 $936x+657y=9$ 的一组解。

关于最小公倍数，我们有如下性质。

引理3 设 a 和 b 是非零整数。则：

（1）a 和 b 的每个公倍数均是 $[a, b]$ 的倍数。

（2）若 m 为正整数，则 $[ma, mb]=m[a, b]$。

（3）$[a, b](a, b)=|ab|$。

证明 （1）令 S 为 a 和 b 的所有公倍数构成的集合。可以象引理1那样证明 S 恰好是由某个正整数 D 的所有倍数构成的集合，显然 D 应当是 S 中的最小正整数，即应当是 $[a,b]$，这

就表明 a 和 b 的每个公倍数均为 $[a, b]$ 的倍数。

(2) 显然 $ma \mid m[a, b]$，$mb \mid m[a, b]$，即 $m[a,b]$ 是 ma 和 mb 的公倍数，由(1)即知 $[ma, mb] \mid m[a,b]$。另一方面，若 d 是 ma 和 mb 的公倍数，则 $m \mid d$。令 $d=md'$，则 $a \mid d'$，$b \mid d'$。于是 $[a, b] \mid d'$，从而 $m[a, b] \mid d$。特别地取 $d=[ma, mb]$，则 $m[a, b] \mid [ma, mb]$。于是 $m[a, b] = [ma, mb]$。

(3) 不妨设 a，b 均为正整数。先设 $(a, b)=1$，根据定义知有 c，$d \in Z$，使 $ca=[a, b]=db$。于是 $b \mid ca$。但是 $(a, b)=1$，从而 $b \mid c$，因此 $ab \mid ac=[a, b]$。但是 ab 是 a 和 b 的公倍数，并且 $ab \mid [a, b]$，所以 ab 就是 a 和 b 的最小公倍数，即 $[a, b]=ab$。因此当 $(a, b)=1$ 时，$(a,b)[a, b]=1 \cdot ab=ab$。

对于一般情形，令 $d=(a,b)$，则 $\frac{a}{d}$ 和 $\frac{b}{d}$ 互素，上面已经证明了 $\left(\frac{a}{d}, \frac{b}{d}\right)\left[\frac{a}{d}, \frac{b}{d}\right]=\frac{a}{d} \cdot \frac{b}{d}=\frac{ab}{d^2}$，于是 $(a,b)[a,b]$

$=d\left(\frac{a}{d}, \frac{b}{d}\right) \cdot d\left[\frac{a}{d}, \frac{b}{d}\right]=d^2 \cdot \frac{ab}{d^2}=ab$。证毕。

习 题 一

1．设 a，b 都是正整数，证明

$$(a, b)=[a, b] \Longleftrightarrow a=b。$$

2．(1) 对于每个奇数 n，证明：$8 \mid (n^2-1)$。

(2) 对于每个整数 n，证明：$4 \nmid (n^2+2)$。

3．设 n，k 为大于 1 的正整数，则

$$(n-1)^2 \mid n^k-1 \Longleftrightarrow (n-1) \mid k。$$

4．证明：连续 n 个整数之积被 $n!$ 除尽。

5．设 $n>1$ 为奇数，证明

$$n \mid \left(1+\frac{1}{2}+\cdots+\frac{1}{n-1}\right)\cdot(n-1)!。$$

6．设 m，n 为正整数，证明：在 n，$2n$，…，mn 这 m 个数中恰有 (m, n) 个被 m 整除。

7．设 n 是正整数，证明：$\frac{21n+4}{14n+3}$ 是既约分数。

8．设 m，n 为正整数，m 是奇数，证明：2^m-1 和 2^n+1 互素。

9．设 m，n 为正整数，证明

$$(2^m-1,\ 2^n-1)=2^{(m,n)}-1。$$

10．设 m，n 为正整数，$m>2$，证明：$2^m-1 \nmid 2^n+1$。

11．证明：首项系数为1的整系数多项式 $f(x)=x^n+\alpha_1 x^{n-1}+\cdots+\alpha_{n-1}x+\alpha_n$ 的有理根必为整数。

12．(1) 设 n 是正整数，则 $\sqrt{n}$ 是有理数 $\Longleftrightarrow$ n 是完全平方数。

(2) 设 S 是有理数集的子集，S 中任意两个不同数的积都是整数，证明：S 中任意 k 个不同数的积也是整数，$k\geqslant 2$。

13．设 α_1，…，α_n 为实数，n 为正整数，证明：

(1) $[\alpha_1]+\cdots+[\alpha_n] \leqslant [\alpha_1+\cdots+\alpha_n] \leqslant [\alpha_1]+\cdots+[\alpha_n]+n-1$。

(2) $\left[\frac{[n\alpha]}{n}\right]=[\alpha]$。

14．设 α，β 为实数，证明：$[2\alpha]+[2\beta] \geqslant [\alpha]+[\beta]+[\alpha+\beta]$。

15．给出定理 1 的一个不同证明。

16. 设 n 为正整数，证明：有唯一的一对整数 k，l，使 $n=\frac{k(k-1)}{2}+l$，其中 $0\leqslant l<k$。

17.（1）对任意正整数 n，有唯一的一对整数 q，r，使得 $n=q^2+r$，其中 $0\leqslant r\leqslant 2q$。

（2）求出所有使 $[n]\mid n$ 的正整数 n。

18. 证明：当 $n=1, 2, \cdots$，时，$[(1+\sqrt{2})^n]$ 轮流取偶、奇数。

19. 设 $\alpha=k+\frac{1}{2}+\sqrt{k^2+\frac{1}{4}}$，这里 k 是给定的正整数，证明：对 $n\geqslant 1$，$k\mid [\alpha^n]$。

20. 设 $\alpha_1, \cdots, \alpha_n$ 是不全为零的整数，$b\in Z$，证明：方程 $\alpha_1x_1+\cdots+\alpha_nx_n=b$ 有整数解的充要条件是 $(\alpha_1, \cdots, \alpha_n)\mid b$。

21. 求下列方程的一组整数解：

（1）$243x+198y=909$。

（2）$41x-114y=5$。

22. 求 $[243, 198]$。

23. 求 $(25, 9, 45)$。

§ 2 算术基本定理

每个大于 1 的正整数 n 均有因子 1 和 n，其他正因子均叫 n 的**真因子**。例如4有真因子2，而 3 没有真因子。如果 d 是 n 的真因子，则 $n=cd$，易知 c 也是 n 的真因子. 于是 n 就分解成两个正整数之积，并且 $1<c$，$d<n$。如果 c 或者 d 还有真因子，则这种分解再继续下去，一直到 $n=n_1n_2\cdots n_r$，而每个 n_i 均没有真因子时为止。所以，对于正整数的分解来说，那些没有真因子的

正整数是不能再分解的“基石”。

定义 设 p 为大于 1 的正整数，如果 p 没有真因子（即只有 1 和 p 是 p 的正因子），则 p 叫作**素数**（或质数），否则便叫作**合数**。

于是，正整数共分成三大类：1，素数，合数。

100 以内的素数有25个：2，3，5，7，11，13，17，19，23，29，31，37，41，43，47，53，59，61，67，71，73，79，83，89，97。

若 p 为素数，n 为任意整数，则由素数定义不难看出：

$$(p, n)=\begin{cases}1, & \text{如果 } p\nmid n。\\ p, & \text{如果 } p\mid n。\end{cases}$$

素数的另一个重要性质是

引理 4 设 p 是素数而 α_1，α_2，…，α_n 为整数。如果 $p\mid\alpha_1\alpha_2\cdots\alpha_n$，则 p 必除尽某个 α_i（$1\leqslant i\leqslant n$）。

证明 如果 $n=1$，则 $p\mid\alpha_1$，取 $i=1$ 即可。当 $n=2$ 时，即 $p\mid\alpha_1\alpha_2$。如果 $p\mid\alpha_1$，则证毕；如果 $p\nmid\alpha_1$，则 $(p, \alpha_1)=1$，因此 $p\mid\alpha_2$，所以 $n=2$ 时命题也成立。对于一般的 n 用数学归纳法即可证明。

现在我们证明初等数论中最基本的一个结果。

算术基本定理 每个大于 1 的正整数 n 均可分解成有限个素数之积，并且若不计素因子的次序，这个分解式是唯一的。

证明 我们先证分解式的存在性。如果 $n=2$，则 2 为素数，从而 2 本身就是所求的分解式，现在设小于 n 的每个正整数均可分解。考虑 n，如果 n 是素数，则证毕。否则 n 便有真因子 d，而 $n=cd$，其中 c 和 d 均是大于 1 的正整数，并且 c，d 均小于 n。由归纳假设，c 和 d 均有分解式 $c=p_1p_2\cdots p_t$，$d=q_1q_2\cdots q_s$，其中 p_1，…，p_t，q_1，…，q_s 均是素数。因此 $n=cd=p_1\cdots p_tq_1\cdots q_s$ 就是所求的分解式。

再证唯一性。当 $n=2$ 时，分解式显然是唯一的。现在设比 n

小的正整数其分解式均是唯一的。考虑正整数 n，设 $n=p_1p_2\cdots p_l$，$n=q_1q_2\cdots q_s$ 是 n 的两个素因子分解式，其中 $p_1,\cdots,p_l$，$q_1,\cdots,q_s$ 均是素数，则 $p_1\mid n=q_1\cdots q_s$。根据引理4，p_1 必整除某个 q_i（$1\leqslant i\leqslant s$）。不妨设 $i=1$，即 $p_1\mid q_1$，即 p_1 为 q_1 的因子。但是 q_1 为素数而 $p_1>1$，因此 $p_1=q_1$。所以令 $n'=\frac{n}{p_1}=\frac{n}{q_1}$，则 $n'=p_2\cdots p_l$，$n'=q_2=q_s$。如果 $n'=1$，则 $n=p_1=q_1$，即 n 的分解式唯一。如果 $n'>1$，注意 $n'<n$，从而由归纳假设，n' 只有唯一的分解式。从而必然有 $l=s$，并且（不妨设）$p_2=q_2$，$\cdots$，$p_l=q_l$，再由 $p_1=q_1$ 即知 n 分解式也是唯一的。证毕。

注记 将 n 的分解式中相同素因子收集在一起，可知每个大于1的正整数 n 均可唯一写成

$$n=p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r},$$

其中 p_1，p_2，$\cdots$，p_r 是**彼此不同**的素数，而 $e_1,\cdots,e_r$ 均为正整数。这叫作 n 的**标准分解式**。例如，$4200=2^3\cdot3\cdot5^2\cdot7$。

我们说过，素数是整数的“基石”，所以对素数的研究是数论的一个重要课题。第一个问题自然是：素数是否有无穷多个。公元前3世纪，欧几里德就证明了

定理 素数有无穷多个。

证明 用反证法。假若素数只有有限多个，令 p_1，p_2，$\cdots$，p_r 是全部素数。考虑大于1的正整数 $n=p_1p_2\cdots p_r+1$。根据算术基本定理，n 是有限个素数之积：$n=q_1\cdots q_l$，于是 $q_1\mid n$。但是已假定全部素数只有 $p_1,\cdots,p_r$，所以 q_1 必是某个 p_i。但由 $n=p_1\cdots p_r+1$ 可知 $p_i\nmid n$（$1\leqslant i\leqslant r$），从而 $q_1\nmid n$。这就导致矛盾，因此素数有无穷多个。证毕。

人们发现，素数在正整数中的分布是很不规则的。例如，对于每个正整数 $n\geqslant2$，连续 $n-1$ 个正整数 $n!+2$，$n!+3$，$\cdots$，$n!+n$ 都不是素数（为什么？）。所以在正整数序列中，可以有

任意长的一段区间中不包含素数。另一方面，任意两个相邻正整数 n 和 $n+1$（$n\geqslant 3$）中必有一个是大于2的偶数，所以不是素数。所以相邻两数均为素数的只有 2 和 3 。但是 n 和 $n+2$ 均为素数的则有很多。这样的一对素数叫作**孪生素数对**。例如在 100 以内有七对孪生素数：（3，5），（5，7），（11,13），（29，31），（41，43），（59，61），（71，73）。猜想有无穷多对孪生素数，但至今未能证明。

我们以 $\pi(x)$ 表示不超过 x 的素数的个数（其中 x 为任意正实数）。我们已经证明了素数有无穷多个，这相当于 $\lim\limits_{x\to+\infty}\pi(x)=+\infty$。不超过 x 的正整数个数显然是 $[x]$ 。所以素数在正整数中所占的比例为 $\dfrac{\pi(x)}{[x]}$。可以证明

$$\lim_{x\to+\infty}\frac{\pi(x)}{[x]}=\lim_{x\to+\infty}\frac{\pi(x)}{x}=0\text{。}$$

这表明：虽然素数有无穷多，但是素数在正整数中的分布是稀疏的。进一步还可证明

$$\lim_{x\to+\infty}\frac{\pi(x)}{\dfrac{x}{\ln x}}=1\text{（素数定理）。}$$

1742年6月7日，普鲁士驻俄国公使，数学家哥德巴赫（Goldbach）在给他的朋友，俄籍瑞士数学家欧拉（Euler）的信中，提出了“每个大于 2 的偶数均是两个素数之和”这一著名的猜想。这个问题目前以我国数学家陈景润的结果为最好。有人验证了：对于 3.3×10^6 以内的偶数，哥德巴赫猜想都正确。但这个猜想至今未能解决。

如果有了正整数 a，b 的素因子分解式，就很容易写出它们的最大公因子和最小公倍数。

引理 5　设