惠阳师专教材

基础数论

陈宏基编

惠阳师专数学系

前　言

本讲义为惠阳师专数学系数论课程而编写．数论知识对未来的数学教师是十分有用的，所有的师范院校的数学专业都应开设这门课程．本讲义作为一个学期的教材使用，它所需要的基础知识并不多，只要有初等代数和初等微积分，以及简单高等代数和解析几何知识就足够了．因此，学生可在任一学期选修这一门课．

讲义详细介绍了整除、同余、不定方程、连分数等初等数论的基本内容，在第二章附加介绍数论函数，重点是狄利克雷卷积下函数集合的代数结构．另外第八章的几何数论，简单介绍了用几何研究数论的方法．素数定理的初等证明比较冗长，限于篇幅，未编进来．

学数论的最好方法是动手去做练习，而数论的习题往往是较困难的．因此，我尽可能地多编进些例题和习题，读者学习时应把习题和课文同样重视．事实上习题本来就是教材的一部分，是教材的补充、深化和提高，同时练习中一些习题往往比课文的内容更有趣些．多做数论习题能使学生得到严格的数学训练，这无疑是十分有益的．

我要感谢何文端付教授，他阅完全部原稿并提出宝贵的建议．还有容树坤同志为我刻写了全部原稿，教务科和打字室全体同志为及时印出讲义付出了辛勤劳动，在此一并致谢．

由于水平有限，错误难免，欢迎批评指正．

陈宏基

1985年12月于惠州

目 录

第一章 整数的整除法

在这一章里，先采扼要地介绍整数整除理论．主要内容包括两个方面，一是介绍初等数论中的基本概念，例如整除、最大公因数和最小公倍数、素数和合数等；另一方面证明算术基本定理，它对以后各章都十分重要．此外还要介绍欧几里得算法，这是一种求最大公因数的有效方法．

§1. 整除性

我们用$\mathbb{Z}$表示整数集．就是

$$\mathbb{Z}=\{\cdots,-3,-2,-1,0,1,2,3,\cdots\}$$

用$\mathbb{Z}^+$表示正整数．$\mathbb{Z}=\{1,2,3,\cdots\}$

[定义] 设$a,b\in\mathbb{Z}$，若存在$c\in\mathbb{Z}$，使得$ac=b$．我们就说a是b的约数（或因数），b是a的倍数，叫做a整除b．用记号$a|b$表示．而用记号$a\nmid b$表示a不能整除b．

若$ac=b$，且$a\neq b$，$a\neq 1$．则a叫做b的真约数．即b的约数中非b非1者，叫做b的真约数．

注意．若$a|b$，$b\neq 0$，那么$a\neq 0$；同样地，若$a|b$，$a=0$，那么$b=0$．然而，若$b=0$，无论对每一个$a\in\mathbb{Z}$，都有$a|b$．从定义出发，我们容易导出下面的定理．

[定理1.1] (i) $\forall a\in\mathbb{Z}$，有$a|a$．

(ii) 若$a|b$，$b|a$，则$a=\pm b$．

(iii) 若$a|b$，$b|c$，则$a|c$．

(iv) 若$a|b$，$a|c$，则$a|(bx+cy)$，其中$x,y\in\mathbb{Z}$．

[证明] (i)、(ii)、(iii)留作练习，这里只证明(iv)．由于$a|b$，$a|c$，

根据定义，存在 $d、e\in Z$，使 $ad=b$，$ae=c$. 那么对任意的 x、$y\in Z$，有 $bx+cy=a(dx+ey)$，而 $dx+ey\in Z$，所以 $a|(bx+cy)$.

[定理1.2] 若 $b\neq 0$，$a|b$，则 $|a|\leq|b|$.

[证明] 由于 $a|b$，根据定义，存在 $c\in Z$，使得 $ac=b$，那么，$|a||c|=|b|\neq 0$，得出 $|c|\neq 0$. 显然 $|c|\geq 1$，故 $|a|\leq|a||c|=|b|$.

[定理1.3]（带余除法）若 $a,b\in Z$，$b\neq 0$，则存在一对 q、$r\in Z$，使得 $a=bq+r$，$0\leq r<|b|$. 且这 q，r 是唯一的.

[证明] 因为 a 必在数列

$$\cdots,-2|b|,-|b|,0,|b|,2|b|,\cdots$$

中相邻两数之间，我们不妨假定

$$q|b|\leq a<(q+1)|b|,$$

于是，$a-q|b|\geq 0$，$a-q|b|<|b|$. 令 $a-q|b|=r$，那么 $0\leq r<|b|$. 因此当 $b>0$ 时，我们有 $a=qb+r$；当 $b<0$ 时，我们有 $a=(-q)b+r$. 这样，我们就证明了 q、r 的存在性；下面我们来证明它们的唯一性.

假如 $a=q_1b+r_1$，$0\leq r_1<|b|$，那么

$$(q-q_1)b=r_1-r,\quad 0\leq|r_1-r|<|b|$$

即 $|q-q_1|\cdot|b|<|b|$，因此 $|q-q_1|<1$. 但 q、q_1 都是整数，则 $q-q_1=0$，所以 $q=q_1$，于是 $r=r_1$. 这就是说 q，r 是唯一的. 定理证毕.

上述定理中的 r 叫做 b 除 a 得到的最小非负余数或简称余数，当 $r=0$ 时，$a=qb$，那么 a 就是 b 的倍数了.

例1. 证明四个连续整数的乘积加1必定是一个平方数.

证明：设 a 是第一个整数，则

$$\begin{aligned}&a(a+1)(a+2)(a+3)+1\\&=(a^2+3a)(a^2+3a+2)+1\\&=[(a^2+3a+1)-1][(a^2+3a+1)+1]+1\\&=(a^2+3a+1)^2-1+1\end{aligned}$$

$= (a^2+3a+1)^2$

因为 a^2+3a+1 是一个整数，所以 $a(a+1)(a+2)(a+3)+1$ 是一个平方数．

例2　n 为非负整数，证明 $7^{n+2}+8^{2n+1}$ 恒为 57 的倍数．

证明：当 $n=0$ 时，$7^2+8=57$，命题成立．

当 $n>0$ 时，$7^{n+2}+8^{2n+1} = 49\cdot 7^n + 8\cdot 64^n$

$= 57\cdot 7^n + 8\cdot 64^n - 8\cdot 7^n$

$= 57\cdot 7^n + 8(64^n - 7^n)$

由于 $n\in Z^+$，所以 $64-7 \mid (64^n-7^n)$

故得 $57 \mid 7^{n+2}+8^{2n+1}$

例3　若 $n\in Z^+$，$n>1$，则 $S=\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$ 不是整数．

证明：令 2^k 表示不超过 n 的 2 的最高次幂，$2^k \le n < 2^{k+1}$，将

$S=\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{n}$

通分，其公分母必为 $2^k m$，m 为奇数。通分后，$\frac{1}{2^k}$ 这一项的分子为奇数 m，而其余各项之分子均为偶数（都至少乘上一个 2），所以其和之分子为奇数，而分母为偶数，因此，S 不是整数．

练习

1．证明定理 1.1 (i) (ii) (iii)．

2．说明若 $b=0$ 时定理 1.2 不一定成立．

3．假设 φ 是一个集，R 是 φ 上的一个关系。若 $r, s\in\varphi$，我们记 rRs 是指 r 通过关系 R 与 s 对应。关系 R 若满足下面条件就称 R 为 φ 上的一个偏序。

(1) 对于任意 $s\in\varphi$，sRs．

(2) 若 rRs，sRr，则 $r=s$．

(3) 若 rRs，sRt，则 rRt．

证明 "$\mid$" 是 Z^+ 上的一个偏序：

4．用数学归纳法证明，若 $a \mid b_i$ $(i=1,2,\cdots,n)$，那么对任意

的 $x_i \in \mathbb{Z}$ $(i=1, 2, \cdots n)$，$a \mid \sum_{i=1}^{n} b_i x_i$.

1-5. 假定 $a, b \in \mathbb{Z}^+$ 且 $ab=C$，证明 $a \leq \sqrt{C}$ 或 $b \leq \sqrt{C}$ 至少一个成立.

1-6. 若 n 是不等于 ± 1 的奇数，证明 n 不能同时整除两个连续的偶数. n 也不能同时整除两个连续的奇数.

1-7. 假设 a，b，$n \in \mathbb{Z}$ 且 $|a-b| < |n|$. 证明 n 不能同时整除 a 和 b.

1-8. 假设 $a \in \mathbb{Z}$，证明

(1) 对于任意的 $n \in \mathbb{Z}$，$a \mid n$ 当且仅当 $a = \pm 1$.

(2) 对于任意的 $n \in \mathbb{Z}$，$n \mid a$ 当且仅当 $a = 0$.

1-9. 设 $a, b, C \in \mathbb{Z}$，且 $C \neq 0$，说明由 $ac \mid bc$ 可推出 $a \mid b$.

1-10. 对于任意的 $n \in \mathbb{Z}$，证明 $3 \mid (n+1)(n+2)n$.

1-11. 证明对于任意的 $n \in \mathbb{Z}$，$\frac{n^3}{3} - \frac{n^2}{2} + \frac{n}{6}$ 是整数.

1-12. n 为非负整数，证明 $3^{2n+3} + 40n - 27$ 是 6 的倍数.

1-13. 若 $n \in \mathbb{Z}^+$，证明 $S = \frac{1}{3} + \frac{1}{5} + \cdots + \frac{1}{2n+1}$ 不是整数.

§2. 最大公因数和最小公倍数

上节我们是讨论一个数的约数、倍数，这节我们来讨论若干个数的约数、倍数.

[定义] 若 a、b、$d \in \mathbb{Z}$，且 $d \mid a$，$d \mid b$，那么 d 称为 a、b 的公因数.

显然，对任意给定的一对整数，它们至少都有两个公因数 1 和 -1. 假若这对整数 a、b 至少有一个不为 0，它们的公因数只有有穷多个.

[定义] 若 a，$b \in \mathbb{Z}$，且 a，b 不同时为 0，若整数 d 满足

(1) $d \in \mathbb{Z}^+$;

(2) d 是 a，b 的一个公因数;

(3) 若 e 是 a、b 的任一公因数，则 $e \mid d$.

那么称 d 为 a 和 b 的最大公因数，用 (a,b) 表示。

例如，$(4,12)=4$，$(2,3)=1$，$(6,8)=2$。两个不同时为0的整数的最大公因数存在不是很明显的事实，我们将在下面定理证明。然而，若最大公因数存在的话，易知它是唯一的，因为，若 $d=(a,b)$ 和 $e=(a,b)$，那么由定义中的条件(3)有 $e|d$ 和 $d|e$，又根据(1)，d 和 e 都是正的，所以 $d=e$。

[定理2.1] 若 a，b 为不同时为0的整数，那么 (a,b) 存在且等于集

$$\varphi=\{au+bv : u、v\in Z\}$$

的最小正整数。(a,b) 整除 φ 的任一元素。特别地，存在 x，$y\in Z$，使得 $(a,b)=ax+by$。

[证明] 显然有 $\pm a=a(\pm 1)+b(0)$，$\pm b=a(0)+b(\pm 1)$。所以 $\pm a$，$\pm b\in\varphi$，而 $\pm a$，$\pm b$ 至少有一个是正整数，所以 φ 包含有正整数，根据自然数的最小数原理，则 φ 必含有一个最小的正整数 d。设 $d=au_0+bv_0$，我们再证明 $d=(a,b)$。

设 $c=au_1+bv_1$ 是 φ 中的任一个元素，存在 q，$r\in Z$，使 $c=dq+r$ $0\le r<d$。现证 $r\in\varphi$。因为

$$\begin{aligned} r=c-dq &=(au_1+bv_1)-(au_0+bv_0)q \\ &=a(u_1-u_0q)+b(v_1-v_0q) \end{aligned}$$

但 $r<d$，这意味着 $r=0$，因为 d 是 φ 中的最小的正整数。所以 $c=dq$。这就证明了对于任意的 $c\in\varphi$，$d|c$。

因为 a，$b\in\varphi$，我们有 $d|a$，$d|b$，那么 d 满足了最大公因数定义的条件(1)、(2)；我们现在来证明它满足条件(3)。假设 $e|a$，$e|b$，由定理1.1(iv)，e 整除 a 和 b 的任意线性组合。但 d 是 a，b 的一个线性组合，所以 $e|d$，则 $d=(a,b)$，证毕。

关于定理2.1中的集 φ，我们可以进一步讨论。在上面我们已经说明了若 $c\in\varphi$，那么 $d|c$；反之也对。即，若 $d|c$，那么 $c\in\varphi$。因为若 $d|c$，那么必存在 $n\in Z$，使得 $dn=c$。根据定理2.1，我们

有 $d=ax+by$，所以 $c=dn=a(xn)+b(yn)\in\mathcal{Y}$. 这就证明了下面的推论.

[推论2.1a] 假设 a、b、$c\in\mathbb{Z}$，a，b 不同时为 0 且 $d=(a,b)$，$d|c$ 当且仅当存在 u，$v\in\mathbb{Z}$，使得 $c=au+bv$.

[定义] 若 a，$b\in\mathbb{Z}$，a，b 不同时为 0，且 $(a,b)=1$，称 a 和 b 互素.

易知存在整数 u，v 使得 $au+bv=1$. 相反地，如果存在 u，$v\in\mathbb{Z}$，使得 $au+bv=1$，由推论 2.1a 得，$(a,b)|1$，又因为 $(a,b)>0$，故 $(a,b)=1$. 所以我们得到下面的

[推论2.1b] $(a,b)=1$ 的充要条件是存在 u，$v\in\mathbb{Z}$，使得 $au+bv=1$.

由上述的结论容易得出下面两个定理.

[定理2.2] 若 $(a,b)=d$，则 $\left(\frac{a}{d},\frac{b}{d}\right)=1$.

[证明] 设 $d=(a,b)$，那么存在 x，$y\in\mathbb{Z}$，使得 $d=ax+by$，所以 $1=\frac{a}{d}x+\frac{b}{d}y$.

而 $\frac{a}{d}$，$\frac{b}{d}\in\mathbb{Z}$，由推论 2.1b 得 $\left(\frac{a}{d},\frac{b}{d}\right)=1$.

[定理2.3] 若 $a|bc$ 且 $(a,b)=1$，则 $a|c$.

[证明] 由 $(a,b)=1$，则存在 x，$y\in\mathbb{Z}$，使得 $ax+by=1$. 那么，$acx+bcy=1$. 但 $a|ac$ 且 $a|bc$，所以根据定理 1.1 (iv) 得 $a|c$.

[定义] 设 a，$b\in\mathbb{Z}$，$ab\neq0$，整数 m 满足

(1) $m\in\mathbb{Z}^+$，

(2) $a|m$，$b|m$，

(3) 若 $a|n$ 且 $b|n$，则 $m|n$.

称 m 是 a 和 b 的最小公倍数，用 $<a,b>$ 表示.

例如，$<4,12>=12$，$<2,3>=6$，$<6,8>=24$. 易见任

意一对非0的整数 a，b 的最小公倍数 $<a,b>$ 是普遍存在的，而且它且它是下面集合的最小正元素

$$\varphi=\{n: n\in\mathbb{Z}^+, a|n, b\in n\}$$

因为 $|ab|\in\varphi$，存在一个最小的正整数 $m\in\varphi$，显然 m 满足(1)和(2)。假设 $n\in\mathbb{Z}$ 且 $a|n$，$b|n$，我们找 q、r 使得 $n=mq+r$，$0\le r<m$，由于 $a|n$，$a|m$，所以 $a|r$。同样地，$b|r$，所以 $r\in\varphi$ 或 $r=0$。由 m 的选择可知 $r=0$。因此 $m|n$，即 m 满足(3)，故 $m=<a,b>$。

下面的定理给出了两个非0整数的最大公因数和最小公倍数之间的关系。

[定理 2.4] 假设 $ab\neq0$，那么 $(a,b)<a,b>=|ab|$。

[证明] 假设 $(a,b)=d$ 和 $<a,b>=m$。我们要证 $ab|dm$ 和 $dm|ab$。我们首先看到 $d|ab$（因为 $d|a$）和 $m|ab$（因为 $a|ab$，$b|ab$）。也就是 $\frac{ab}{d}\in\mathbb{Z}$，$\frac{ab}{m}\in\mathbb{Z}$。

由于 $d|b$，所以 $ad|ab$，或 $a|\frac{ab}{d}$。同样有 $b|\frac{ab}{d}$。所以 $m|(\frac{ab}{d})$ 或 $dm|ab$，但 $b|m$，所以 $ab|am$，或 $(\frac{ab}{m})|a$。同样地，$(\frac{ab}{m})|b$，所以 $(\frac{ab}{m})|d$ 或 $ab|dm$。所以，$dm=\pm ab=|ab|$。证毕。

练习

2-1. 证明：(1) $(ac,bc)=|c|(a,b)$；

(2) 若 $a|c$，$b|c$，且 $(a,b)=1$，那么 $ab|c$；

(3) $(a,b)=|a|$ 当且仅当 $a|b$；

(4) 若 $(a,b)=1$ 且 $(a,c)=1$，则 $(a,bc)=1$。

2-2. 证明：

(1) $<ac,bc>=|c|<a,b>$；

(2) $<a,b>=|a|$ 当且仅当 $b|a$。

2-3. 证明：

(1) 若 $(a,b)=(a,c)$ 且 $<a,b>=<a,c>$，则 $a=\pm c$；

(2) $\langle a,(b,c)\rangle=(\langle a,b\rangle,\langle a,c\rangle)$;

(3) $(a,\langle b,c\rangle)=\langle(a,b),(a,c)\rangle$.

2-4. 证明定理2.2的逆定理：如果 $0<d$，$d|a$，$d|b$ 且 $(\frac{a}{d},\frac{b}{d})=1$，那么 $(a,b)=d$.

2-5. 两个以上整数的最大公因数定义如下：若 $a_1,\cdots,a_n\ (n\geq 2)$ 不全为0，它们的最大公因数 $(a_1,\cdots,a_n)=d$ 是满足下面条件的唯一的正整数：$d|a_i\ (i=1,\cdots,n)$ 且若 $e|a_i\ (i=1,\cdots,n)$. 那么 $e|d$. 用数学归纳法证明当 $n>2$，$(a_1,\cdots,a_n)=((a_1,\cdots,a_{n-1}),a_n)$.

2-6. 两个以上非0整数的最小公倍数 $m=\langle a_1,\cdots,a_n\rangle$ 是满足如下条件的唯一正整数：$a_i|m\ (i=1,2,\cdots,n)$，且若 $a_i|M\ (i=1,\cdots,n)$，那么 $m|M$. 证明当 $n>2$，$\langle a_1,\cdots,a_n\rangle=\langle\langle a_1,\cdots,a_{n-1}\rangle,a_n\rangle$.

2-7. 如果 $(a,b)=1$，我们知道存在整数 u,v 使得 $au+bv=1$. 证明：$(u,v)=(b,u)=(a,v)=1$.

2-8. 若 $b\neq 0$，$a=bq+r$，$0\leq r<|b|$，证明 $(a,b)=(b,r)$.

2-9. 举例说明方程 $(a,b)=ax+by$ 的解不是唯一的。

2-10. 指出 $(a,b)=\langle a,b\rangle$ 的充要条件.

2-11. 证明对于 $\forall n\in\mathbb{Z}$，$(3,n^2+1)=1$，$(5,n^2+2)=1$，$(7,n^2+2)=1$.

2-12. 若 $a,b,n\in\mathbb{Z}^+$ 且 $n>1$，指出 n^a-1 和 n^b-1 的最大公约数和最小公倍数.

2-13. 假设 $f(x)$ 是一个次数 ≥ 1 的整系数多项式. 如果方程 $f(x)=0$ 有一个有理根 $\frac{a}{b}$，$b\neq 0$，$(a,b)=1$，证明 a 整除 $f(x)$ 的常数项，而 b 整除 $f(x)$ 的首项系数. 由此推证 $\sqrt{2}$ 不是有理数.

§3. 欧几里得算法

我们已经证明了两个不同时为0的最大公因数的存在性和唯一性. 这一节我们介绍一种求最大公因数的有效方法. 这种方法是由我国古代数学家最先创造出来的. 但是由于历史的原因, 在一般的书称它为欧几里得算法. 这种方法的理论根据是带余除法.

[定理3.1] (欧几里得算法) 设 a, b 为任意两个正整数. 作带余除法, 得下面一串等式:

$$a = bq_1 + r_1 \quad , \quad 0 \le r_1 < b$$

$$b = r_1 q_2 + r_2 \quad , \quad 0 \le r_2 < r_1$$

$$r_1 = r_2 q_3 + r_3 \quad , \quad 0 \le r_3 < r_2$$

$$\cdots\cdots\cdots\cdots\cdots\cdots$$

则对足够大的 n, 必有

$$r_{n-1} = r_n q_{n+1} + r_{n+1} \quad , \quad r_{n+1} = 0$$

且 $(a, b) = r_n$.

[证明] 由作法可知, 数列

$$b \ , \ r_1 \ , \ r_2 \ , \ r_3 \ , \cdots$$

是非负单调下降的. 所以, 这些余数中最终必会出现0, 假定 $r_{n+1} = 0$ 那么就有 $r_{n-1} = r_n q_{n+1} + r_{n+1}$, $r_{n+1} = 0$.

再反复应用练习2-8, 可得

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = (r_n, 0) = r_n.$$

例1. 计算 (245, 1022)

解: $1022 = 245 \cdot 4 + 42$

$245 = 42 \cdot 5 + 35$

$42 = 35 \cdot 1 + 7$

$35 = 7 \cdot 5$

所以 $(245, 1022) = 7$.

例2 计算 (299, 247), 并求出一对 x, y 使

$(299, 247) = 299x + 247y$.

解： $299 = 247 \cdot 1 + 52$

$247 = 52 \cdot 4 + 39$

$52 = 39 \cdot 1 + 13$

$39 = 13 \cdot 3$

所以 $(299, 247) = 13$. 由倒数第二等式可得

$$13 = 52 - 39 \cdot 1$$

依次倒推上去，就有

$$13 = 52 - 39 \cdot 1 = 52 - (247 - 52 \cdot 4)$$

$$= -247 + 52 \cdot 5 = -247 + (299 - 247 \cdot 1)5$$

$$= 299 \cdot 5 + 247(-6)$$

于是 $x = 5$, $y = -6$ 为所求的一对整数.

练习

3-1. 求 $(20, 35)$, $(112, 96)$.

3-2. 用欧几里得算法求下面式子的 x , y .

$(20, 35) = 20x + 35y$; $(112, 96) = 112x + 96y$.

3-3. 求 $<20, 35>$, $<112, 96>$.

3-4. 用练习2-5和欧几里得算法求：

(1) $(60, 30, 42, 8)$;

(2) $(2250, 30, 540, 900)$.

3-5. 用练习2-6和定理2.4 求.

(1) $<60, 30, 42, 8>$;

(2) $<2250, 30, 540, 900>$.

3-6. 证明定理3.1中的 $n \leq \dfrac{2\log b}{\log 2}$.

§4 素数·算术基本定理

在正整数里，1的正因数只有它本身，因此在整数中间1占有特殊的地位．任一个大于1的整数，都至少有两个正因数，即1和它本身．除此之外，也可能还有别的正因数．例如4的正因数除了1和4之外，还有正因数2，但5的正因数就只有1和5，再没有别的正因数了．

[定义] 一个大于1的正整数，如果它的正因数只有1和它本身，这样的正整数叫做素数（或质数）；否则就叫做合数．

例如 2、3、5、7、…都是素数，而4、6、8、9、10…都是合数．

由素数和合数的定义可知，全体正整数可分为三类：(1) 1；(2)全体素数；(3)全体合数．

素数在研究整数的过程中占有一个很重要的地位，本节主要目的就是要证明任何一个大于1的整数，如果不论次序，能唯一地表成素数的乘积．我们先证明每一个大于1的整数有一素因数，即

[定理4.1] 若$a\in\mathbb{Z}^+$，$a>1$，则a除1外最小正因数q是一个素数，并且a是合数时，$q\le\sqrt{a}$．

[证明] 假定q不是素数，由定义，q有因数q_1，$1<q_1<q$，但$q\mid a$，所以$q_1\mid a$．这与q是a的除1外的最小正因数矛盾，故q是素数．

当a是合数时，则$a=a_1q$，且$a_1>1$，否则a是素数．由于$q$$a$除1外的最小正因数，所以$q\le a_1$，$q^2\le qa_1=a$，故$q\le\sqrt{a}$．

[定理4.2] 若p是一素数，a是任一整数，则$p\mid a$或$(p,a)=1$．

[证明] 若$p\nmid a$，令$d=(p,a)$．则$d\mid p$，故$d=1$或$d=p$．但$d\mid a$而$p\nmid a$，故$d\neq p$，因而$d=1$，即$(p,a)=1$．

[推论4.2] 设$a_1, a_2, \cdots a_n$是n个整数，p是素数，若$p|a_1a_2\cdots a_n$，则p至少能整除某一a_k.

[证明] 对n用数学归纳法.

当$n=2$，$p|a_1a_2$，若$p|a_1$结论成立，假设$p\nmid a_1$，那么$(p,a_1)=1$，根据定理2.3，我们有$p|a_2$.

假定对$n-1$个数的乘积定理成立，我们来证明对n个数的乘积亦成立. 事实上，由$p|a_1a_2\cdots a_n$，即$p|a_1(a_2\cdots a_n)$，若$p|a_1$，结论成立，若$p\nmid a_1$，则$p|a_2\cdots a_n$. 根据归纳假设$a_2, \cdots a_n$这$n-1$个数中至少有一个a_k能被p整除. 证毕.

[定理4.3](算术基本定理) 若$n>1$，那么，n可以分解有限多个素数的乘积，并且若不考虑素因子的排列次序时，分解式是唯一的.

[证明](存在性) 当$n=2$，定理显然成立.

假定定理对$<n$的所有整数成立，我们来证明对n亦成立. 若n是素数，定理自然成立. 若n不是素数，那末它有一个因数d，$1<d<n$. 设$de=n$，那么$1<e<n$. 由归纳假设，d和e都可分解为有限个素数的乘积，从而n也可以分解成有限个素数的乘积.

(唯一性) 我们再一次用数学归纳法来证. 当$n=2$，显然因子分解式是唯一的. 假设对$<n$的所有整数分解式都是唯一的. 若n是素数，分解式自然是唯一的. 若n是合数，假设n有两种形式的素因子分解式：$n=p_1\cdots p_r$和$n=q_1\cdots q_k$，其中$p_i(i=1,\cdots r)$和$q_j(j=1,\cdots,s)$是素数；因为n不是素数，显然r和s都大于1. 由$p_1\cdots p_r=q_1\cdots q_s$，我们有$p_1|q_1\cdots q_s$，由推论4.2，存在$K, 1\le K\le s$使得$p_1|q_k$，得$p_1=q_k$.

又由于$\frac{n}{p_1}<n$和$1<p_2\cdots p_r=\frac{n}{p_1}$，所以$\frac{n}{p_1}=\frac{n}{q_k}$都有唯一的素因子分解式，因此$r=s$，且对任意的$i$，$i=2,\cdots,r$总存在$j$，$i\neq k$，$1\le j\le s$，使$p_i=q_j$，因而$\frac{n}{p_1}=p_2\cdots p_r$是唯一的，那么$n=p_1p_2\cdots p_r$就是唯一素因子分解式. 证毕.