普通高等教育信息安全类国家级特色专业系列规划教材

信息安全数学基础

（第二版）

聂旭云　廖永建　熊　虎　编著

科学出版社

普通高等教育信息安全类国家级特色专业系列规划教材

信息安全数学基础

（第二版）

聂旭云　廖永建　熊　虎　编著

科学出版社

北京

内 容 简 介

本书系统地介绍了网络空间安全研究所涉及的数论、抽象代数相关内容以及信息论、复杂度理论的初步理论，具体包括：整除、同余、同余方程；群、环、域、多项式、有限域及椭圆曲线的概念及性质；保密系统的信息理论；计算复杂度理论等。在介绍这些数学理论的同时，围绕着大整数的运算、有限域的元素表示及其运算给出了部分计算机实现算法的设计，为后续密码算法的实现提供了参考。

本书具有较大的参考价值，非常适合于工程人才培养，可作为高等院校网络空间安全、信息安全等专业本科生或研究生教材，也可作为计算机、通信工程及电子商务等专业的参考书，还可供信息安全相关工程技术人员参考。

图书在版编目(CIP)数据

信息安全数学基础 / 聂旭云，廖永建，熊虎编著. —2 版. —北京：科学出版社, 2019.6

普通高等教育信息安全类国家级特色专业系列规划教材

ISBN 978-7-03-061207-6

Ⅰ. ①信… Ⅱ. ①聂… ②廖… ③熊… Ⅲ. ①信息安全－应用数学－高等学校－教材 Ⅳ. ①TP309 ②O29

中国版本图书馆 CIP 数据核字(2019)第 092667 号

责任编辑：潘斯斯 刘 博 王晓丽 / 责任校对：王 瑞

责任印制：张 伟 / 封面设计：迷底书装

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京虎彩文化传播有限公司 印刷

科学出版社发行 各地新华书店经销

*

2013 年 2 月第 一 版 开本：787×1092 1/16

2019 年 6 月第 二 版 印张：11

2019 年 6 月第五次印刷 字数：250 000

定价：59.00 元

(如有印装质量问题，我社负责调换)

前　言

本书第一版自出版以来一直在电子科技大学投入本科教学使用。在教学过程中，作者发现对于工科院校的学生来说，算法的原理与实现是学生关注的重点，也是提高学生实践能力的途径之一。因此，作者对本书第二版做了如下修订。

修订后，全书还是分为 10 章。第 1 章、第 2 章和第 3 章的内容属于初等数论，系统地介绍了整除、同余、二次剩余等原理和相关算法。与第一版相比， 第 1 章增加了部分例题，增加了“多精度数平方算法”。原书第 2 章拆分成了两章，增加了“RSA 公钥加密算法”，拆分出来的第 3 章为“同余方程”，增加了“模 p 的平方根算法”和“Rabin 公钥加密算法”。第 4 章和第 5 章为代数系统，详细地介绍了群、环、域的基本概念和性质，增加了“原根”的概念和“ElGamal 公钥加密算法”。第 6 章着重介绍了多项式及多项式中的一些运算算法，为学习有限域的知识作出了铺垫。第 7 章为有限域，给出了有限域的结构定理和有限域的构造方法，并对有限域上运算的实现进行了探讨，增加了“多项式的阶或周期”的概念。第 8 章对椭圆曲线的相关知识进行了介绍，并给出了双线性对的定义和计算方法的介绍，增加了椭圆曲线上的“大步小步算法”描述以及“椭圆曲线的 ElGamal 公钥加密算法”。第 9 章主要介绍了保密系统的信息理论，主要是信息熵、互信息以及相关性质。第 10 章主要介绍了复杂度理论相关概念，主要有时间复杂度、空间复杂度、P 问题和 NP 问题等。原书的第 10 章“组合数学”，与其他章节关联不大，因此这次修订时将这章删去了。

本书修订工作主要由聂旭云完成，由廖永建和熊虎负责审阅和校对。

在本书的修订和出版过程中，得到了电子科技大学信息与软件工程学院秦志光教授和周世杰教授的大力支持和指导，在此对他们表示感谢。

由于作者水平有限，书中疏漏和不当之处难免，欢迎大家批评指正。对于本书的任何问题请发送 E-mail 到作者邮箱 xynie@uestc.edu.cn。

作　者

2019 年 2 月

目　录

第 1 章　整　　除

数论是一门非常重要的数学基础课，是研究整数最基本性质的一门学科。数论在信息安全、计算机科学等现代重要科技领域有着重要的应用。本章主要介绍整数的整除概念及其相关性质和算法设计。

通常，用 $\mathbb{Z}$ 表示整数集合，整数即

$$0, \pm 1, \pm 2, \cdots$$

自然数就是非负整数，用 $\mathbb{N}$ 来表示。

1.1　整除概念和基本性质

定义 1.1.1（整除）　设 $a,b \in \mathbb{Z}$，$a \neq 0$。如果存在某个整数 $q \in \mathbb{Z}$，使得 $b = aq$，则称 a 整除 b 或 b 被 a 整除，记为 $a \mid b$，且称 a 为 b 的因数，b 为 a 的倍数。

显然，0 是任何整数的倍数。对于任意整数 a，$\pm 1, \pm a$ 都是它的因数，称这四个因数为整数 a 的显然因数或平凡因数，整数 a 的其他因数称为非显然因数或非平凡因数。

例 1.1.1　(1) $28 = 4 \times 7$，因此 $4 \mid 28$，$7 \mid 28$，4 和 7 为 28 的因数，28 为 4 和 7 的倍数。

(2) $-3 \mid 18$，因为 $18 = (-3) \times (-6)$。

(3) $173 \mid 0$，因为 $0 = 173 \times 0$。

由整除的定义和乘法运算的性质，可以推导出整除关系有如下性质。

定理 1.1.1（整除的性质）　对任意的 $a,b,c \in \mathbb{Z}$，有

(1) 如果 $a \mid b$ 且 $b \mid c$，则有 $a \mid c$。

(2) 如果 $a \mid b$ 且 $a \mid c$，当且仅当对于任意 $x, y \in \mathbb{Z}$，有 $a \mid bx + cy$。

(3) 设 $m \neq 0$，$a \mid b$ 当且仅当 $ma \mid mb$。

(4) 如果 $a \mid b$ 且 $b \mid a$，则 $a = \pm b$。

证明： (1) $a \mid b$ 且 $b \mid c$，则存在整数 q_1，q_2，使得 $b = aq_1, c = bq_2$，因此有 $c = aq_1q_2$，所以 $a \mid c$。

(2) 必要性：$a \mid b$ 且 $a \mid c$，则存在整数 q_1，q_2，使得 $b = aq_1, c = aq_2$。因此有 $bx + cy = a(q_1x + q_2y)$，所以 $a \mid bx + cy$。

充分性：分别取 $x = 1, y = 0$ 和 $x = 0, y = 1$，即可得 $a \mid b$ 且 $a \mid c$。

(3) 当 $m \neq 0$ 时，$b = aq \Leftrightarrow mb = (ma)q$。

(4) $a \mid b$ 且 $b \mid a$，则存在整数 q_1，q_2，使得 $b = aq_1, a = bq_2$，因此有 $a = a(q_1q_2)$。又因为 $a \neq 0$，所以 $q_1q_2 = 1$。由于 q_1，q_2 是整数，所以 $q_1 = \pm 1$，故而 $b = \pm a$。　□

定理 1.1.2（带余除法）　设 a,b 是两个给定的整数，$a \neq 0$，那么一定存在唯一的一对整数 q 和 r，满足

$$b=aq+r,\quad 0\leqslant r<|a|$$

因此，$a|b$ 的充要条件是 $r=0$。

证明：存在性。当 $a|b$ 时，取 $q=\dfrac{b}{a}$，$r=0$。当 $a\nmid b$ 时，考虑集合

$$T=\{b-ka,k=0,\pm1,\pm2,\cdots\}$$

容易看出，集合 T 中必有正整数，取 T'为 T 的正整数子集。由于正整数集合的任一非空子集均有最小正整数。因此，T'中必然存在一个最小正整数，设为

$$t_0=b-k_0a>0$$

下证 $t_0<|a|$。因为 $a\nmid b$，所以 $t_0\neq|a|$。若 $t_0>|a|$，则有 $t_1=t_0-|a|\in T$，且 $0<t_1<t_0$。这与 t_0 的极小性矛盾，因此有 $t_0<|a|$。取 $q=k_0$，$r=t_0$ 就满足要求。　□

定理 1.1.2 中的 q 称为 a 除 b 的不完全商，记为 $a\operatorname{div}b$，r 称为 a 除 b 的余数，记为 $a\bmod b$。

定义 1.1.2（公因数）　设 a_1,a_2,d 是三个整数，若 $d|a_1,d|a_2$，则称 d 是整数 a_1,a_2 的公因数。一般地，设 $a_1,a_2,\cdots,a_k$ 是 k 个整数，若 $d|a_1,d|a_2,\cdots,d|a_k$，称 d 是整数 $a_1,a_2,\cdots,a_k$ 的公因数。

例如，$a_1=12,a_2=8$，它们的公因数是 $\pm1,\pm2,\pm4$。

定义 1.1.3（最大公因数）　设 a_1,a_2 是两个不全为零的整数，把 a_1,a_2 的公因数中最大的正整数称为 a_1和 a_2 的最大公因数，记为 $\gcd(a_1,a_2)$ 或简记为 (a_1,a_2)。当 $(a_1,a_2)=1$ 时，称 a_1,a_2 互素。一般地，设 $a_1,a_2,\cdots,a_k$ 是 k 个不全为零的整数，把 $a_1,a_2,\cdots,a_k$ 的公因数中最大的正整数称为 $a_1,a_2,\cdots,a_k$ 的最大公因数，记为 $\gcd(a_1,a_2,\cdots,a_k)$ 或简记为 $(a_1,a_2,\cdots,a_k)$。当 $(a_1,a_2,\cdots,a_k)=1$ 时，称 $a_1,a_2,\cdots,a_k$ 互素。

等价地，(a_1,a_2) 是能够同时整除 a_1,a_2 的最大正整数。

例 1.1.2　(1) 12 与 18 的公因数有 $\{\pm1,\pm2,\pm3,\pm6\}$，所以 $(12,18)=6$。

(2) -15 与 21 的公因数有 $\{\pm1,\pm3\}$，所以 $(-15,21)=3$。

(3) 25 与 12 的公因数有 ±1，所以 $(25,12)=1$，因此 25 与 12 互素。

定理 1.1.3（最大公因数的性质）　对于任意整数 a，b，c，有

(1) $(a,b)=(b,a)=(-a,b)=(a,-b)$；

(2) 若 $a|b$，则 $(a,b)=a$；

(3) 对于任意两个整数 x,y，必有 $(a,b)|ax+by$；

(4) 若 $a=bq+c$，q 是一个整数，则有 $(a,b)=(b,c)$；

(5) 若 $(a,c)=1$，$b|c$，则 $(a,b)=1$；

(6) $\left(\dfrac{a}{(a,b)},\dfrac{b}{(a,b)}\right)=1$。

证明：根据最大公因数的定义，很容易得出 (1)，(2)。根据定理 1.1.1 整除的性质 (2)，立刻可得 (3)。根据最大公因数的定义及整除的性质，很容易得出 $(a,b)|(b,c)$，$(b,c)|(a,b)$，因此结论 (4) 成立。

(5) 设 $(a,b)=d$，则由 $d|b$，$b|c$，可得 $d|c$，又 $d|a$，所以 $d|(a,c)$。由 $(a,c)=1$，可得 $d=1$，即 $(a,b)=1$。

(6) 设$(a, b)=d$，$\left(\frac{a}{d},\frac{b}{d}\right)=d'$，由$d'|\frac{a}{d}, d'|\frac{b}{d}$，可得$dd'|a$，$dd'|b$，根据最大公因数的性质可知$dd'|d$，由此可得$d'=1$，结论得证。 □

定义 1.1.4(公倍数) 设a_1,a_2,l是三个整数，若$a_1|l, a_2|l$，则称l是整数a_1,a_2的公倍数。一般地，设$a_1,a_2,\cdots,a_k$是k个整数，若$a_1|l, a_2|l,\cdots,a_k|l$，称$l$是整数$a_1,a_2,\cdots,a_k$的公倍数。

定义 1.1.5(最小公倍数) 设a_1,a_2是两个不全为零的整数，把a_1,a_2的所有公倍数中的最小正整数称为整数a_1和a_2的最小公倍数，记为 $\mathrm{lcm}[a_1,a_2]$或简记为$[a_1,a_2]$。一般地，设$a_1,a_2,\cdots,a_k$是 k 个不全为零的整数，把$a_1,a_2,\cdots,a_k$的所有公倍数中的最小正整数称为整数$a_1,a_2,\cdots,a_k$的最小公倍数，记为 $\mathrm{lcm}[a_1,a_2,\cdots,a_k]$或简记为$[a_1,a_2,\cdots,a_k]$。

等价地，$[a_1,a_2]$是能够被a_1和a_2同时整除的最小正整数。

定理 1.1.4 设a，b，m是整数，$a|m$，$b|m$，则 $[a, b]|m$。

证明： 不妨设$m=q[a, b]+r$，其中q是整数，$0\leqslant r<[a,b]$，则$r=m-q[a, b]$，又$a|m$，$b|m$，$a|[a, b]$，$b|[a, b]$，由整除的性质可知$a|r$，$b|r$，由$[a, b]$的最小性可知$r=0$。因此有$[a, b]|m$。 □

1.2 欧几里得算法及其扩展算法

本节考虑如何求出两个整数的最大公因数。

求最大公因数的算法称为辗转相除法，也称为欧几里得算法，主要工具是带余除法。

设a和b是两个整数，不妨设$a>b$，$b\neq 0$，依次做带余数除法：

$$\begin{aligned}
a&=bq_1+r_1, && 0<r_1<|b|\\
b&=r_1q_2+r_2, && 0<r_2<r_1\\
&\vdots\\
r_{k-1}&=r_kq_{k+1}+r_{k+1}, && 0<r_{k+1}<r_k\\
&\vdots\\
r_{n-2}&=r_{n-1}q_n+r_n, && 0<r_n<r_{n-1}\\
r_{n-1}&=r_nq_{n+1}+r_{n+1}, && r_{n+1}=0
\end{aligned}\tag{1.1}$$

经过有限步运算，必然存在n使得$r_{n+1}=0$，这是因为

$$0\leqslant r_{n+1}<r_n<\cdots<r_1<|b|$$

欧几里得算法的描述如算法 1.2.1。

算法 1.2.1 计算两个整数的最大公因数的欧几里得算法。

输入：两个非负整数a，b，且$a\geqslant b$。

输出：a，b的最大公因数。

1. 当$b\neq 0$时，作

   $r\leftarrow a \bmod b, a\leftarrow b, b\leftarrow r$。

2. 返回(a)。

定理 1.2.1 设a，b是两个整数，不妨设$a>b$，则$(a, b)=r_n$，其中r_n是上述辗转相除法中得到的最后一个非零余数。

证明：根据最大公因数的性质(4)，有

$$\begin{aligned}(a,b)&=(b,r_1)\\&=(r_1,r_2)\\&\vdots\\&=(r_{n-1},r_n)\\&=r_n\end{aligned}$$

□

例 1.2.1　计算(4864,3458)。

解：做辗转相除法

$$\begin{aligned}4864&=1\times3458+1406, & q_1&=1,r_1=1406\\3458&=2\times1406+646, & q_2&=2,r_2=646\\1406&=2\times646+114, & q_3&=2,r_3=114\\646&=5\times114+76, & q_4&=5,r_4=76\\114&=1\times76+38, & q_5&=1,r_5=38\\76&=2\times38, & q_6&=2,r_6=0\end{aligned}$$

所以$(4864,3458)=r_5=38$。

注意当 a，b 中有负整数时，可根据最大公因数的性质(1)将其中的负整数转变为正整数来求其最大公因数。

例 1.2.2　用辗转相除法求(–123, 17)。

解：(–123, 17) = (123, 17)

做辗转相除法：

$$\begin{aligned}123&=7\times17+4, & q_1&=7,\ r_1=4\\17&=4\times4+1, & q_2&=4,\ r_2=1\\4&=1\times4, & q_3&=1,\ r_3=0\end{aligned}$$

因此，$(123,17)=r_2=1$。

定理 1.2.2　对于任意两个整数 a，b，存在整数 x，y 使得

$$(a,\ b)=xa+yb。$$

证明：根据辗转相除法，有

$$\begin{aligned}r_1&=a-bq_1\\r_2&=b-r_1q_2=-q_2a+(1+q_1q_2)b\end{aligned}\tag{1.2}$$

一般地，对于任意的 r_i，都存在两个整数 x_i，y_i，使

$$r_i=x_ia+y_ib$$

x_i，y_i 可利用下述递推公式得到：

$$\begin{aligned}r_i&=r_{i-2}-q_ir_{i-1}\\&=(x_{i-2}a+y_{i-2}b)-q_i(x_{i-1}a+y_{i-1}b)\\&=(x_{i-2}-q_ix_{i-1})a+(y_{i-2}-q_iy_{i-1})b\end{aligned}\tag{1.3}$$

可见

$$x_i=x_{i-2}-q_ix_{i-1},\quad y_i=y_{i-2}-q_iy_{i-1},\quad i=1,2,3,\cdots$$

由式(1.2)可知

$$x_{-1}=1,\quad x_0=0$$
$$y_{-1}=0,\quad y_0=1$$

利用这几个初始值及递推关系式(1.3)，就可依次计算出$(x_1,y_1),(x_2,y_2),\cdots,(x_n,y_n)$，最后得到

$$(a,b)=r_n=x_na+y_nb$$

令$x=x_n$，$y=y_n$，定理得证。 □

定理 1.2.2 的证明过程中给出的计算 x，y 的算法称为扩展的欧几里得算法，如算法 1.2.2 所示。

算法 1.2.2 扩展的欧几里得算法。

输入：两个非负整数 a，b，且$a\geqslant b$。

输出：$d=(a,b)$与满足$ax+by=d$的整数 x 与 y。

1．若$b=0$，则$d\leftarrow a,x\leftarrow 1,y\leftarrow 0$，返回$(d,x,y)$。

2．设$x_2\leftarrow 1,x_1\leftarrow 0,y_2\leftarrow 0,y_1\leftarrow 1$。

3．当$b>0$时，作

3.1 $q\leftarrow\lfloor a/b\rfloor,r\leftarrow a-qb,x\leftarrow x_2-qx_1,y\leftarrow y_2-qy_1$；

3.2 $a\leftarrow b,b\leftarrow r,x_2\leftarrow x_1,x_1\leftarrow x,y_2\leftarrow y_1,y_1\leftarrow y$。

4．$d\leftarrow a,x\leftarrow x_2,y\leftarrow y_2$，返回$(d,x,y)$。

注： $\lfloor a/b\rfloor$表示小于等于 a/b 的最大整数。

例 1.2.3 求整数 x，y，使(4864，3458) = 4864x+3458y。

解： 根据例 1.2.1，有

$$\begin{aligned}38&=114-76\\&=114-(646-5\times 114)\\&=-646+6\times(1406-2\times 646)\\&=6\times 1406-13\times(3458-2\times 1406)\\&=-13\times 3458+32\times(4864-3458)\\&=32\times 4864-45\times 3458\end{aligned}$$

因此整数 x = 32，y = –45 满足(4864，3458) = 4864x+3458y。

根据算法 1.2.2，求 x，y 的过程可列成表 1.1。

表 1.1 扩展的欧几里得算法

q	r	x	y	a	b	x_2	x_1	y_2	y_1
–	–	–	–	4864	3458	1	0	0	0
1	1406	1	–1	3458	1406	0	1	1	–1
2	646	–2	3	1406	646	1	–2	–1	3
2	114	5	–7	646	114	–2	5	3	–7
5	76	–27	38	114	76	5	–27	–7	38
1	38	32	– 45	76	38	–27	32	38	– 45
2	0	–91	128	38	0	32	–91	– 45	128

推论 1.2.1　对于任意整数 a，b，c，若 $c|a$ 且 $c|b$，则 $c|(a,b)$。

证明：根据定理 1.2.2，可知存在整数 x，y 使得 $(a,b)=xa+yb$。

根据最大公因数的性质(4)，有 $c|xa+yb$，因此有 $c|(a,b)$。　□

定理 1.2.3　设 a，b 是两个不全为 0 的整数，则 $(a,b)=1$ 当且仅当存在整数 u，v 使得

$$ua+vb=1。$$

证明：必要性是定理 1.2.1 的特例。下证充分性。

如果存在整数 u，v，使得

$$ua+vb=1$$

则根据整除的性质有 $(a,b)|ua+vb$，即有 $(a,b)|1$，因此有 $(a,b)=1$。　□

推论 1.2.2　设 a，b，c 为不等于 0 的整数，

(1)若 $c|ab$，$(a,c)=1$，则 $c|b$；

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

(3)若 $(a,c)=1$，$(b,c)=1$，则 $(ab,c)=1$。

证明：(1)因为 $(a,c)=1$，根据定理 1.2.3 存在整数 u，v，使得

$$ua+vc=1$$

两边同时乘以 b 可得

$$uab+vcb=b$$

由于 $c|uab+vcb$，因此 $c|b$。

(2)由 $(a,b)=1$ 可知存在整数 u，v 使得

$$ua+vb=1$$

两边同时乘以 c，可得

$$uac+vbc=c$$

由于 $a|c$，$b|c$，所以 $ab|uac$，$ab|vbc$。因此有 $ab|c$。

(3)根据定理 1.2.3，存在整数 s，t 使得

$$sa+tc=1$$

同理，存在整数 u，v，使得

$$ub+vc=1$$

于是有

$$(sa+tc)(ub+vc)=(su)ab+(sva+tub+tvc)c=1$$

根据定理 1.2.3 有 $(ab,c)=1$。　□

推论 1.2.3　设 a，b 是两个正整数，

(1)若 a，b 互素，则 $[a,b]=ab$。

(2)$[a,b]=\dfrac{ab}{(a,b)}$。

证明：(1)显然 ab 是 a，b 的公倍数。

设 m 为 a，b 的任意公倍数即 $a|m$，$b|m$。存在整数 k 使得 $m=ak$。由 $b|m$，可知 $b|ak$，又 a，b 互素，由推论 1.2.2 可知 $b|k$。因此存在整数 t 使得 $k=bt$，所以 $m=abt$。故 $ab|m$。由此

可知 ab 是 a，b 的公倍数中的最小正整数，即$[a,\ b]=ab$。

(2)显然$a\mid\dfrac{ab}{(a,b)}$，$b\mid\dfrac{ab}{(a,b)}$，所以$\dfrac{ab}{(a,b)}$是 a，b 的公倍数。

设$a=k_a(a,b)$，$b=k_b(a,b)$，由定理 1.1.3 可知$(k_a,k_b)=1$。设 m 为 a，b 的任意公倍数即 $a|m$，$b|m$。存在整数q_a,q_b，使得$m=q_aa=q_bb$，于是$m=q_ak_a(a,b)=q_bk_b(a,b)$。因此有$q_ak_a=q_bk_b$。由于$(k_a,k_b)=1$，于是有$k_a\mid q_b$，$k_ab\mid q_bb$，$\dfrac{(a,b)k_ab}{(a,b)}\mid q_bb=m$，即$\dfrac{ab}{(a,b)}\mid m$，这表明$\dfrac{ab}{(a,b)}$是 a，b 的最小公倍数。 □

例 1.2.4 求 4864 和 3458 的最小公倍数。

解： 由例 1.2.1 可知(4864，3458) = 38。

因此，$[4864,3458]=\dfrac{4864\times3458}{38}=442624$。

1.3 素数与算术基本定理

素数是整数中的重要组成部分，也可以看作整数构成的最小单元。素数在密码学特别是公钥密码学中有着重要的应用。本节主要介绍素数的基本概念和算数基本定理。

定义 1.3.1(素数) n 是一个整数，且$n\neq0,n\neq\pm1$，若 n 只有平凡因数，则称整数 n 为素数，否则称为合数。

例如，2，3，5，7，11 为素数，4，6，8，10 为合数。

由于当整数$n\neq0,n\neq\pm1$，n 和 $-n$ 必同为素数或合数，所以本书后续若没有特别说明，素数总是指正数。

定理 1.3.1 设 p 是一个素数，a，b 为任意整数。

(1)若 $p\nmid a$，则 p 与 a 互素；

(2)若 $p|ab$，则 $p|a$ 或 $p|b$。一般地，若 $p\mid a_1a_2\cdots a_k$，则必然存在某个 i，$p\mid a_i$ 成立。

证明： (1)设$(p,\ a)=d$，则有 $d\mid p,d\mid a$。因为 p 是素数，所以由 $d\mid p$ 可得 $d=p$ 或 $d=1$。对于 $d=p$，由 $d\mid a$ 可得 $p|a$，与 $p\nmid a$ 矛盾。因此，$d=1$，即 p 与 a 互素。

(2)若 $p|a$ 则定理成立。若 $p\nmid a$ 成立，则 p 与 a 互素，由 1.2 节推论 1.2.2 可知 $p|b$。对于一般情形可以类推。 □

定理 1.3.2(算术基本定理) 任何不为 1 的正整数 n 均可唯一地表示为有限个素数的幂的乘积，即

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$$

其中 $p_1<p_2<\cdots<p_k$，$\alpha_1,\alpha_2,\cdots,\alpha_k$ 是正整数。上式称为 n 的标准分解式。算术基本定理又称为整数分解唯一性定理。

证明： (存在性)若 n 是素数，定理显然成立。

若 n 不是素数，设 p_1 是 n 的最小非平凡正因数，则 p_1 是素数，因为 p_1 的非平凡正因数也是 n 的非平凡正因数，所以 p_1 没有非平凡正因数。设$n=p_1n_1$ $(1<n_1<n)$，对 n_1 重复上述

推理，可得 $n=p_1n_1=p_1p_2n_2$（p_2 是素数，$1<n_2<n_1$）。以此类推，得 $n>n_1>n_2>\cdots>1$，其步骤不超过 n，最后必有

$$n=p_1p_2\cdots p_l$$

将上式中相同素数合并为素数的方幂，并按定理要求排列，就得到了分解的存在性。

（唯一性）设 n 可分解为

$$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}=q_1^{\beta_1}q_2^{\beta_2}\cdots q_l^{\beta_l}$$

其中，$p_1<p_2<\cdots<p_k$，$q_1<q_2<\cdots<q_l$ 都是素数。根据定理 1.3.1，存在某个 q_i 满足 $p_1\mid q_i$，不妨设为 q_1，因为 p_1 和 q_1 都为素数，所以 $p_1=q_1$。类似地，可依次得到 $p_i=q_i$，$2\leqslant i\leqslant k$，因此有 $k=l$。又若 $\alpha_1>\beta_1$，则

$$p_1^{\alpha_1-\beta_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}=p_2^{\beta_2}\cdots p_k^{\beta_k}$$

上式左边被 p_1 整除，右边不能被 p_1 整除，矛盾，所以 $\alpha_1>\beta_1$ 不成立。同理 $\alpha_1<\beta_1$ 也不成立。故 $\alpha_1=\beta_1$。类似可证明 $\alpha_i=\beta_i$，$2\leqslant i\leqslant k$。定理得证。 □

推论 1.3.1　若 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，$b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$，其中 $\alpha_i\geqslant 0,\beta_i\geqslant 0$，则有

$$(a,b)=p_1^{\min(\alpha_1,\beta_1)}p_2^{\min(\alpha_2,\beta_2)}\cdots p_k^{\min(\alpha_k,\beta_k)}$$

和

$$[a,b]=p_1^{\max(\alpha_1,\beta_1)}p_2^{\max(\alpha_2,\beta_2)}\cdots p_k^{\max(\alpha_k,\beta_k)}$$

证明留给读者。

事实上，给定一个大整数，找到其素因子分解并不是一件容易的事。

定义 1.3.2（整数分解问题）　整数分解问题指的是给定一个整数 n，找到其素因子分解，即将 n 写成 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$ 的形式。

整数分解问题目前并没有太好的算法来解决，常见的算法有试除法，即用小于 $\sqrt{n}$ 的素数去试除 n，直到找到 n 的所有素因子。最坏情形下，需要进行 $\sqrt{n}$ 次试除。当 n 比较大时，这种方法的效率并不高。当被分解的整数 n 是某种特殊的形式时，一些分解算法可以具有更高的性能；这些算法通常被称为“特殊目的”分解算法。这些算法有 Pollard rho 算法、Pollard p-1 算法、椭圆曲线算法和特殊数域筛法等，有兴趣的读者可参阅 Menezes 编著的《应用密码学手册》。

关于素数的个数，有如下结论。

定理 1.3.3　素数有无穷多个。

证明：用反证法。

假设只有有限多个素数，设它们为 $p_1,p_2,\cdots,p_k$，令

$$M=p_1p_2\cdots p_k+1$$

任何一个 p_i，$1\leqslant i\leqslant k$，都不整除 M，所以它们都不是 M 的素因子。由定理 1.3.2，M 总有一个素因子，记为 p，则 $p\neq p_i$，$1\leqslant i\leqslant k$，与假设矛盾。因此素数有无限多个。 □

利用定理 1.3.3 的证明方法还可以证明一些特殊结构的素数有无穷多个。

例 1.3.1　证明形如 $4k-1$ 的素数有无穷多个。

证明： 首先证明形如 $4k-1$ 的整数必有一个形如 $4k-1$ 的素因子。

设 $n=4k-1$，

(1)若 n 是素数，则结论成立。

(2)若 n 是合数，则 n 一定是奇数，因此 n 的素因子为 $4k+1$ 和 $4k-1$ 的形式。若 n 没有形如 $4k-1$ 的素因子，则 n 的素因子都为 $4k+1$ 的形式，那么 n 的形式也一定是 $4k+1$，与 n 的形式为 $4k-1$ 矛盾。因此，n 必有一个形如 $4k-1$ 的素因子。

假设形如 $4k-1$ 的素数有有限个，不妨设为 $q_1,q_2,\cdots,q_t$，令

$$M=4(q_1q_2\cdots q_t)-1$$

则 M 必有一个形如 $4k-1$ 的素因子 q，由于形如 $4k-1$ 的素数有有限个 $q_1,q_2,\cdots,q_t$，因此 q 必为 $q_1,q_2,\ldots,q_t$ 中的 1 个，因而有 $q|M$，$q\mid 4(q_1q_2\cdots q_t)$，即 $q|1$，矛盾。所以形如 $4k-1$ 的素数有无穷多个。 □

寻找素数是一个比较困难的问题，古希腊数学家 Eratosthenes 给出了一种称为 Eratosthenes 筛法的算法可以求出不大于某个正整数 N 的所有素数。其原理基于以下定理。

定理 1.3.4 设 n 是一个正合数，p 是 n 的大于 1 的最小正因数，则 p 是素数且 $p\leqslant\sqrt{n}$。

证明： 由定理 1.3.2 的证明过程可知，p 是素数。

因为 n 是合数，所以存在整数 n_1 使得

$$n=pn_1,\quad 1<p\leqslant n_1<n$$

所以有 $p^2\leqslant n$，即 $p\leqslant\sqrt{n}$。 □

由定理 1.3.4 可得一个整数为素数的判别法则。

定理 1.3.5 设 n 是一个正整数。如果对于所有的素数 $p\leqslant\sqrt{n}$，都有 $p\nmid n$，则 n 是素数。

例 1.3.2 求 100 以内的所有素数。

解： $\sqrt{100}=10$。小于 10 的素数有 2，3，5，7。因此将 1~100 的所有除 2，3，5，7 以外的 2 的倍数，3 的倍数，5 的倍数，7 的倍数删去，剩下的数就是全部不超过 100 的素数，如下所示：

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	37	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	67	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

因此，100 以内的素数有 25 个，分别是 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。

下面介绍两类特殊的素数：Mersenne 素数和 Fermat 素数。

定理 1.3.6　设 $n>1$ 是一个正整数，若 a^n-1 是素数，则 $a=2$，n 是素数。

证明：若 $a>2$，则 $a^n-1=(a-1)(a^{n-1}+\cdots+a+1)$，而 $1<a-1<a^n-1$，故 a^n-1 不是素数。与已知矛盾，因此 $a=2$。

若 $a=2$，而 $n=kl$，$k>1$，$l>1$，则 $2^{kl}-1=(2^k-1)(2^{k(l-1)}+\cdots+2^k+1)$，而 $1<2^k-1<2^n-1$，故 2^n-1 不是素数。与已知矛盾，因此 n 是素数。

定义 1.3.3　设 n 是一个正整数，整数 $M_n=2^n-1$ 称为第 n 个 Mersenne 数。当 $M_p=2^p-1$ 是素数时，M_p 称为 Mersenne 素数，其中 p 是素数。

目前，寻找 Mersenne 素数主要采用计算机搜索的方法。1996 年美国数学家及程序设计师沃特曼编制了一个 Mersenne 素数寻找程序，并把它放在网页上供数学家和数学爱好者免费使用；这就是著名的“互特网 Mersenne 素数大搜索”(GIMPS)项目。1997 年美国数学家及程序设计师库尔沃斯基和其他人建立了“素数网”(PrimeNet)，使分配搜索区间和向 GIMPS 发送报告自动化。现在只要人们去 GIMPS 的主页下载那个免费程序，就可以立即参加 GIMPS 项目来搜寻 Mersenne 素数。

已发现的 Mersenne 素数有 41 个，如表 1.2 所示。

表 1.2　已知 Mersenne 素数

序号	Mersenne 素数	位数	序号	Mersenne 素数	位数
1	M_2	1	22	M_{9941}	2993
2	M_3	1	23	M_{11213}	3376
3	M_5	2	24	M_{19937}	6002
4	M_7	3	25	M_{21701}	6533
5	M_{13}	4	26	M_{23209}	6987
6	M_{17}	6	27	M_{44497}	13395
7	M_{19}	6	28	M_{86293}	25962
8	M_{31}	10	29	M_{110503}	33265
9	M_{61}	19	30	M_{132049}	39751
10	M_{89}	27	31	M_{216091}	65050
11	M_{107}	33	32	M_{756839}	227832
12	M_{127}	39	33	M_{859433}	258716
13	M_{521}	157	34	$M_{1257787}$	378632
14	M_{607}	183	35	$M_{1398269}$	420921
15	M_{1279}	386	36	$M_{2976221}$	895933
16	M_{2203}	664	37	$M_{3021377}$	909526
17	M_{2281}	687	38	$M_{6972593}$	2098960
18	M_{3217}	969	39	$M_{13466917}$	4053946
19	M_{4253}	1281	40	$M_{20996011}$	6320430
20	M_{4423}	1332	41	$M_{24036583}$	7235733
21	M_{9689}	2917			

定理 1.3.7　若 2^n+1 是素数，则 n 一定是 2 的方幂。

证明：若 n 有一个奇素因子 q，令 $n=qr$，则

$$2^{qr}+1=(2^r+1)(2^{r(q-1)}-2^{r(q-2)}+2^{r(q-3)}+\cdots-2^r+1)$$