“十二五”重点图书

研究生系列教材

数论算法

Number Theoretical Algorithm

姜建国　臧明相　编著

西安电子科技大学出版社
http://www.xduph.com

研究生系列教材

数 论 算 法

姜建国　臧明相　编著

西安电子科技大学出版社

内 容 简 介

本书从实用角度出发，介绍数论的有关基础理论、实用算法及其应用。全书共9章，主要内容包括整数的可除性、数论函数、同余及其运算、同余方程、二次同余方程与平方剩余、原根与离散对数、连分数、素性测试和整数分解、有限域等。

本书选材精练，推理严谨，重点突出，例题丰富，习题难易适度，对重点内容从不同角度进行论述，尤其对实用问题举例较多，有利于培养读者利用数论的理论和方法解决实际问题的能力。

本书可作为计算机、通信、信息和网络安全、数学等专业的研究生教材，也可作为相关领域科研人员的参考书。

图书在版编目(CIP)数据

数论算法/姜建国，臧明相编著. —西安：西安电子科技大学出版社，2014.5
研究生系列教材
ISBN 978-7-5606-3302-2

Ⅰ. ① 数… Ⅱ. ① 姜… ② 臧… Ⅲ. ① 数论—研究生—教材 Ⅳ. ① O156

中国版本图书馆CIP数据核字(2014)第086058号

策　　划　李惠萍
责任编辑　王　瑛　李惠萍
出版发行　西安电子科技大学出版社(西安市太白南路2号)
电　　话　(029)88242885　88201467　　邮　　编　710071
网　　址　www.xduph.com　　电子邮箱　xdupfxb001@163.com
经　　销　新华书店
印刷单位　北京京华虎彩印刷有限公司
版　　次　2014年5月第1版　2014年5月第1次印刷
开　　本　787毫米×1092毫米　1/16　印张 23.5
字　　数　479千字
定　　价　39.00元
ISBN 978-7-5606-3302-2/O

XDUP 3594001-1

“十二五”重点图书　研究生系列教材

编审委员会名单

前　言

数论是研究整数性质的一个数学分支，它历史悠久，有着强大的生命力。数论问题叙述简明，“很多数论问题可以从经验中归纳出来，并且仅用三言两语就能向一个行外人解释清楚，但要证明它却远非易事”，因而有人说：“用以发现天才，在初等数学中再也没有比数论更好的课程了”，所以在国内外各级各类的数学竞赛中，数论问题总是占有相当大的比重。

随着科学技术的发展，将经典理论与现代应用相结合已成为发展的一种趋势，故数论的应用领域也逐渐扩展开来，顺应发展趋势，推动数论应用，正是本书的编写目的和出发点。实际上，目前数论的有关理论和方法在计算机、通信等领域有着大量的应用，尤其在信息和网络安全、数字信号处理等方面应用更加广泛，而本书也主要从应用角度出发来研究数论问题，尤其是有关整数运算中实用的方法和具体算法。

本书共分9章，各章的主要内容概括如下：

第1章整数的可除性，主要介绍整除概念及与其相关的问题，如整除的定义及其性质，重点介绍了求最大公因数的有关算法。

第2章数论函数，给出了几种常用数论函数并讨论了其性质，同时介绍了函数的积性和函数的 Dirichlet 乘积等概念及性质。

第3章同余及其运算，介绍了整数按同余的分类、同余条件下幂函数的快速运算算法，给出了不定方程的解法、矩阵的同余运算和同余在信息安全和随机数生成方面的应用实例。

第4章同余方程，介绍了同余方程的概念，讨论了同余方程的解数及解法，给出了一次同余方程组和素数模的同余方程的求解方法及同余方程在秘密共享和数据加密方面的应用实例。

第5章二次同余方程与平方剩余，主要针对特殊的同余方程(即二次同余方程的求解)给出了问题的分类、化简和转换方法，重点介绍了利用勒让德符号和雅可比符号判断方程的可解性和模数为素数时的求解方法。

第6章原根与离散对数，从整数的阶与原根的定义出发，给出了阶的性质、原根及其判断方法与计算方法、n 次剩余以及利用原根解特殊高次方程的方法，最后给出了原根和离散对数在密钥管理、信息加密和随机数生成等方面

的应用。

第7章连分数，介绍了连分数的概念和有关性质，重点介绍了用连分数逼近实数和有理分数的方法。

第8章素性测试和整数分解，主要针对素数的精确判断方法的复杂度问题，介绍了素数的概率测试，以及正整数的分解方法。

第9章有限域，主要讨论与数论相关的群、环、域的概念和性质，重点介绍了同余运算与群、环、域的关系，以及利用同余运算实现有限域的构造等问题。

本书具有如下几个特点：

(1) 紧密结合研究生教学实际和教学大纲，在内容编排上力求深入浅出，循序渐进；在讲解理论和原理的同时，给出了大量例题，并在讲解例题时，重视对解题思路的分析，有利于提高读者独立分析问题和解决问题的能力。

(2) 针对工科研究生教学要求，书中除了数论的理论成果外，还结合实际应用，搜集并整理了相关问题的实用算法，尽力做到与时俱进，重在实用。

(3) 注重教学思想方法的渗透和解题水平的提高。拾众家之所长，精选题目，使例题和习题均具有典型性和代表性。

(4) 本书在撰写时，参阅了国内外大量的相关资料，并凝结了作者十多年来从事研究生“数论算法”课程教学的体会，力求内容新颖，取舍得当。

本书是在西安电子科技大学校内教材“数论算法”的基础上，经过多年的试用，并吸取了老师和学生大量的修改意见，不断完善而成的。

西安电子科技大学出版社对本书的出版给予了热情的关怀和支持，尤其是出版社李惠萍老师对书稿严格把关，在内容的叙述方式上提出了很多有益的建议，使作者深受教益，在此表示感谢。

由于作者水平有限，书中不足之处在所难免，恳请读者批评指正，使本书得以不断改进和完善。

编著者

2013年10月

符 号 说 明

以下符号按其所出现的先后顺序排列：

$\mathbf{Z}$——整数集合。

$a\in S$——元素 a 属于集合 S。

$b\mid a$——b 整除 a，即 $a=bq$。

$b\nmid a$——b 不能整除 a。

$A\Leftrightarrow B$——B 是 A 的充分必要条件(简称充要条件)，或者说结论 A 成立的充分必要条件是条件 B 成立。

$|a|$——当 a 为整数时，表示 a 的绝对值。

a/b 或 $\frac{a}{b}$——当 $a=bq$ 时，表示 q 的值。

$(a)_b$——a 被 b 除所得的非负余数，$0\leqslant(a)_b<b$。

$\lfloor x\rfloor$——下整数函数，即不大于变量 x 的最大整数。

$(a_ka_{k-1}\cdots a_1a_0)_p$——整数的 p 进制表示。

$(a_1,a_2,\cdots,a_n)$——整数 $a_1,a_2,\cdots,a_n$ 的最大公因数。

(a,b)——整数 a 和 b 的最大公因数。

$\mathrm{lb}a$，$\log_2 a$——以 2 为底的 a 的对数。

$a\leftrightarrow b$——将变量 a 与 b 的值互换。

$A\Rightarrow B$——若条件 A 成立，则结论 B 必成立。

$[a,b]$——整数 a 和 b 的最小公倍数。

$[a_1,a_2,\cdots,a_n]$——整数 $a_1,a_2,\cdots,a_n$ 的最小公倍数。

$n=p_1^{a_1}p_2^{a_2}\cdots p_k^{a_k}$——整数 n 的标准(素因数)分解式。

$\tau(n)$——正因数个数函数，即整数 n 的正因数的个数。

$p^a\parallel n$，$\mathrm{pot}_p(n)$，$\mathrm{pot}_p n$——$p^a\mid n$，但 $p^{a+1}\nmid n$。

$\binom{n}{r}$，C_n^r——从 n 个相异元素中不重复地选 r 个元素的组合数，$\mathrm{C}_n^r=\frac{n!}{r!\ (n-r)!}$。

$\lceil x\rceil$——上整数函数，即不小于 x 的最小整数。

$[x]$——四舍五入函数。

P_n^r——从 n 个相异元素中不重复地选 r 个元素的排列数，$\mathrm{P}_n^r=\frac{n!}{(n-r)!}$。

$\varphi(n)$——Euler(欧拉)函数，即 1，2，…，n 中与 n 互素的整数的个数。

$|S|$——当 S 为集合时，表示 S 的阶，即 S 的元素个数。

$\mu(n)$——Möbius(墨比乌斯)函数。

$\odot a_1 a_2 \cdots a_n$——元素 $a_1 a_2 \cdots a_n$ 的圆排列。

$\pi(n)$——素数个数函数，即 1～n 之间的所有素数的个数。

$f(n) * g(n)$——数论函数 $f(n)$ 与 $g(n)$ 的 Dirichlet(狄利克雷)乘积。

$I(n)$—— 单位数论函数，$I(n)=\left\lfloor \frac{1}{n} \right\rfloor$。

$f^{-1}(n)$——数论函数 $f(n)$ 的狄利克雷逆函数。

$n \gg 1$——n 充分大。

$a \equiv b \pmod{m}$——a 与 b 模 m 同余。

$a \not\equiv b \pmod{m}$——a 与 b 模 m 不同余。

a^{-1}——整数 a(对模 m)的逆，即 $aa^{-1} \equiv 1 \pmod{m}$。

$\boldsymbol{A}_{m \times n}$，$(a_{ij})_{m \times n}$，$(a_{ij})$——$m$ 行 n 列矩阵。

$\boldsymbol{\Lambda}$，$\mathrm{diag}\{a_1, a_2, \cdots, a_n\}$——($n$ 阶)对角矩阵。

$\boldsymbol{E}_n$，$\boldsymbol{E}$——(n 阶)单位矩阵。

$\boldsymbol{A}^{-1}$——方阵 $\boldsymbol{A}$ 的模 m 的逆矩阵，即 $\boldsymbol{A}\boldsymbol{A}^{-1} \equiv \boldsymbol{A}^{-1}\boldsymbol{A} \equiv \boldsymbol{E} \pmod{m}$。

$|\boldsymbol{A}|$——当 $\boldsymbol{A}$ 为矩阵时，表示 $\boldsymbol{A}$ 的行列式。

$\tilde{\boldsymbol{A}}$，$\mathrm{adj}\boldsymbol{A}$——方阵 $\boldsymbol{A}$ 的模 m 的伴随矩阵。

$\deg f(x)$，$\partial^{\circ} f(x)$，$\partial^{\circ}[f(x)]$——多项式 $f(x)=a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ 的次数。

$T(f(x); m)$，$T(f; m)$——同余方程 $f(x) \equiv 0 \pmod{m}$ 的解数。

$f'(x)$——多项式 $f(x)$ 的导式。

$\oplus$——异或运算。

$\mathrm{L}(a, p)$，$\left(\frac{a}{p}\right)$——勒让德符号，其中 p 为素数。

$\mathrm{J}(a, m)$，$\left(\frac{a}{m}\right)$——雅可比符号。

$\mathrm{ord}_m(a)$——整数 a 对模数 m 的阶(或指数，乘法周期)。

$\mathrm{dlog}_{m,g}a$，$\mathrm{dlog}_g a$，$\mathrm{dlog}a$，$\mathrm{ind}_g a$，$\mathrm{ind}a$——以 g 为底的整数 a 对模数 m 的离散对数(或对数，指标)。

$a/b \pmod{m}$——同余运算下的除法运算，规定为 $ab^{-1} \pmod{m}$。

$\langle x_0, x_1, \cdots, x_n \rangle$——有限连分数。

$\langle x_0, x_1, x_2, \cdots \rangle$——无限连分数。

$\langle a_0, a_1, \cdots, a_{m-1}, \overline{a_m, \cdots, a_{m+k-1}} \rangle$——循环连分数。

$\boldsymbol{\beta}(m)=(\alpha_1, \alpha_2, \cdots)$——整数 m 的指数向量，其中 m 的分解式为 $m=p_1^{\alpha_1} p_2^{\alpha_2} \cdots (\alpha_i \geqslant 0, i=1, 2, \cdots)$。

$a \notin A$——元素 a 不属于集合 A。

$B \subset A$——集合 B 是集合 A 的子集。

$A \cap B$，AB——集合 A 与集合 B 的交集。

$A \cup B$，$A+B$——集合 A 与集合 B 的并集或和集。

$A-B$——集合 A 与集合 B 的差集。

$A_1 \times A_2 \times \cdots \times A_n$——集合 A_1，A_2，…，A_n 的积集(或 Descartes(笛卡尔乘积))。

$\phi: A_1 \times A_2 \times \cdots \times A_n \to D$，$A_1 \times A_2 \times \cdots \times A_n \xrightarrow{\phi} D$，$\phi: (a_1, a_2, \cdots, a_n) \longrightarrow d$，$(a_1, a_2, \cdots, a_n) \xrightarrow{\phi} d$——由集合 $A_1 \times A_2 \times \cdots \times A_n$ 到 D 的映射。

ϕ^{-1}——映射 ϕ 的逆映射。

$a \circ b$——元素 a 和元素 b 的代数运算。

$A \cong B$——集合 A 与集合 B 同构。

$|G|$——当 G 为群时，表示群 G 的阶。

$|R|$——当 R 为环时，表示环 R 的阶。

$R[x]$——环 R 上所有以 x 为变量的多项式集合。

$\max(a, b)$——最大值函数，即选 a 和 b 中的最大者。

$R_q[x]$——系数属于环 R_q 的多项式集合。

$R_q[x]_{m(x)}$——系数属于环 R_q 中的次数低于 $\partial^\circ m(x)$ 的所有多项式的集合。

$|F|$——当 F 为域时，表示域 F 的阶。

$GF(n)$，GF——Galois(伽罗华)域。

Z_m——集合 $\{0, 1, 2, \cdots, (m-1)\}$。

Z_m^+——集合 $Z_m-\{0\}=\{1, 2, \cdots, (m-1)\}$。

$F[x]$——系数属于域 F 的多项式集合。

$F[x]_{p(x)}$——$F[x]$ 中次数小于 $\partial^\circ p(x)$ 的多项式集合。

$Z_m^* = \{a \mid a \in Z_m, (a, m)=1\}$——集合 Z_m 中与 m 互素的整数构成的集合。

目　　录

第 1 章　整数的可除性

数论这门学科最初是从研究整数开始的，所以也叫整数论。后来整数论又进一步发展成为数论。确切地说，数论是一门研究整数性质的学科。

人类从学会计数开始就一直和自然数打交道，后来由于实践的需要，数的概念进一步扩充，自然数被称做正整数，而把它们的相反数称做负整数，介于正整数和负整数中间的中性数称做 0。它们合起来称做**整数**。

对于整数可以施行加、减、乘、除四种运算，称做**四则运算**。其中加法、减法和乘法三种运算在整数范围内可以毫无阻碍地进行。即任意两个或两个以上的整数相加、相减、相乘时，它们的和、差、积仍然是一个整数。但整数之间的除法在整数范围内并不一定能够无阻碍地进行。

数论算法主要从应用角度出发，研究数论问题，尤其是有关整数运算中实用的方法和技术。

1.1　整除的概念与带余除法

1.1.1　整除及其性质

【定义 1.1.1】　设 a，$b\in\mathbf{Z}$(整数集合)，$b\neq 0$，如果存在 $q\in\mathbf{Z}$，使得 $a=bq$，则称 ***b* 整除 *a*** 或 ***a* 可被 *b* 整除**，记做 $b\mid a$，且称 a 是 b 的**倍数**，b 是 a 的**因数**(也可称为**除数**、**约数**、**因子**)；否则，称 ***b* 不能整除 *a*** 或 ***a* 不能被 *b* 整除**，记做 $b\nmid a$。

【例 1.1.1】　求 30 的所有因数。

解　能够整除 30 的整数有 ±1，±2，±3，±5，±6，±10，±15，±30，故它们都是 30 的因数。

由定义可以直接得到以下简单的结论：

(i) 若 $a=bq$，则 q 也是 a 的因数，并将 q 写为 a/b 或 $\frac{a}{b}$；

(ii) 当 b 遍历整数 a 的所有因数时，$-b$ 也遍历整数 a 的所有因数；

(iii) 当 b 遍历整数 a 的所有因数时，a/b 也遍历整数 a 的所有因数。

例如，设 $a=6$，则有：

(1) 当 $b=3$ 时，$q=2=6/3$ 也是 6 的因数；

(2) 当 $b=1, 2, 3, 6, -1, -2, -3, -6$ 遍历整数 6 的所有因数时，$-b=-1, -2, -3, -6, 1, 2, 3, 6$ 也遍历整数 6 的所有因数；

(3) 当 $b=1, 2, 3, 6, -1, -2, -3, -6$ 遍历整数 6 的所有因数时，$a/b=6, 3, 2, 1, -6, -3, -2, -1$ 也遍历整数 6 的所有因数。

【特例】 以下是关于整除的特殊情形下的结论：

(i) 0 是任何非零整数的倍数；

(ii) ± 1 是任何整数的因数；

(iii) 任何非零整数 a 是其自身的倍数，也是其自身的因数。

整数的整除具有以下性质：

【性质 1.1.1】 设 $a, b\in\mathbf{Z}$，则

$$b\mid a\Leftrightarrow b\mid -a\Leftrightarrow -b\mid a\Leftrightarrow -b\mid -a\Leftrightarrow |b|\mid |a|$$

证 由于这几个结论的证明思路和方法基本上是一样的，故此处只证明“$b\mid a\Leftrightarrow b\mid -a$”，其余结论的证明可以类推(其中 $b\mid a\Leftrightarrow b\mid -a$ 表示 b 整除 $-a$ 是 b 整除 a 的充分必要条件)。

由定义 1.1.1 知，$b\mid a$ 的充要条件是存在整数 q，使得 $a=bq$；而按照整数的四则运算性质知，$a=bq$ 的充要条件是 $-a=(-q)b$；然后再由定义 1.1.1 知，$-a=(-q)b$ 的充要条件是 $b\mid -a$。所以由充要条件的传递性知“$b\mid a\Leftrightarrow b\mid -a$”成立。

【性质 1.1.2】 传递性。设 $a, b, c\in\mathbf{Z}$，若 $c\mid b$ 且 $b\mid a$，则 $c\mid a$。

证 已知 $c\mid b$ 且 $b\mid a$，则由定义 1.1.1 知存在整数 q_1 和 q_2，使得 $b=cq_1$ 且 $a=bq_2$，从而有 $a=(cq_1)q_2=c(q_1q_2)=cq$，且 $q=q_1q_2$ 为整数，故由定义 1.1.1 知 $c\mid a$。

【性质 1.1.3】 设 $a, b, c\in\mathbf{Z}$，若 $c\mid a$ 且 $c\mid b$，则 $c\mid a\pm b$。

证 已知 $c\mid a$ 且 $c\mid b$，则由定义 1.1.1 知存在整数 q_1 和 q_2，使得 $a=cq_1$ 且 $b=cq_2$，从而有 $a\pm b=cq_1\pm cq_2=c(q_1\pm q_2)=cq$，且 $q=q_1\pm q_2$ 为整数，故由定义 1.1.1 知 $c\mid a\pm b$。

【性质 1.1.4】 设 $a, b, c\in\mathbf{Z}$，若 $c\mid a$ 且 $c\mid b$，则对任意整数 s、t，有 $c\mid sa+tb$。

证 与性质 1.1.3 的证明方法相似，已知 $c\mid a$ 且 $c\mid b$，则由定义 1.1.1 知存在整数 q_1 和 q_2，使得 $a=cq_1$ 且 $b=cq_2$。于是，从 $sa\pm tb=s(cq_1)\pm t(cq_2)=c(sq_1\pm tq_2)=cq$ 即可看出 $c\mid sa+tb$。

【推论】 设 $a_1, a_2, \cdots, a_n, b\in\mathbf{Z}$，若 $b\mid a_i (i=1, 2, \cdots, n)$，则对任意整数 $s_1, s_2, \cdots, s_n$，有 $b\Big|\sum_{i=1}^{n}s_ia_i$。

【性质 1.1.5】 设 $a, b\in\mathbf{Z}$，若 $b\mid a$ 且 $a\mid b$，则 $a=\pm b$。

证 已知 $b\mid a$ 且 $a\mid b$，则由定义 1.1.1 知存在整数 q_1 和 q_2，使得 $a=bq_1$ 且 $b=aq_2$，即有 $a=q_1q_2a$，从而 $q_1q_2=1$，$q_1=q_2=\pm 1$，故有 $a=\pm b$。

【性质 1.1.6】 $b\mid a\Leftrightarrow cb\mid ca (c\neq 0)$。

证 必要性：已知 $b\mid a$，由定义 1.1.1 知存在整数 q，使得 $a=bq$，从而有 $ca=cbq$，即

当 $c\neq 0$ 时，有 $cb|ca$。

充分性：已知 $cb|ca$，由定义 1.1.1 知存在整数 q，使得

$$ca=(cb)q$$

而当 $c\neq 0$ 时，上式等价于 $a=bq$，即 $b|a$。

【性质 1.1.7】 若 $b|a$ 且 $a\neq 0$，则 $|b|\leqslant|a|$。

证 由定义 1.1.1 知，若 $b|a$，则 $b\neq 0$，且存在整数 q，使得 $a=bq$。而当 $a\neq 0$ 时，必有 $q\neq 0$，从而 $|q|\geqslant 1$，即 $|b|\leqslant|a|$。

【例 1.1.2】 证明：若 $3|n$ 且 $5|n$，则 $15|n$。

证 由 $3|n$ 知 $n=3m$，所以 $5|3m$。再由 $5|5m$ 和性质 1.1.4 知 $5|(2\cdot 5m-3\cdot 3m)=m$，即 $m=5q$，所以 $n=3(5q)=15q$，因此有 $15|n$。

【例 1.1.3】 设 $a=2t-1$，若 $a|2n$，则 $a|n$。

证 已知 $a=2t-1$，所以 $2t=a+1$。由 $a|2n$ 知 $a|2tn$，又由 $a|an$ 及性质 1.1.3 知

$$a|(2tn-an)=(a+1)\,n-an=n$$

即 $a|n$。

【例 1.1.4】 设 a、b 是两个给定的非零整数，且有整数 x、y，使得 $ax+by=1$。证明：若 $a|n$ 且 $b|n$，则 $ab|n$。

证 由 $ax+by=1$ 得

$$n=n\cdot 1=n(ax+by)=(na)x+(nb)y$$

再由 $a|n$ 且 $b|n$ 知，$ab|na$，$ab|nb$。

所以由性质 1.1.4 知，$ab|x(na)+y(nb)=(ax+by)n=n$，即 $ab|n$。

另外，注意到 $3\cdot 2+5\cdot(-1)=1$，从而也从另一角度证明了例 1.1.2。

【例 1.1.5】 设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 是整系数多项式，若 $d|b-c$，则 $d|f(b)-f(c)$。

证 首先，由多项式的计算性质，易得

$$f(b)-f(c)=a_n(b^n-c^n)+a_{n-1}(b^{n-1}-c^{n-1})+\cdots+a_1(b-c)$$

其次，由 $d|b-c$ 及 $b^k-c^k=(b-c)(b^{k-1}+b^{k-2}c+b^{k-3}c^2+\cdots+c^{k-1})$ 可知 $d|b^k-c^k$ $(k=1,2,\cdots,n)$。

所以由性质 1.1.4 的推论知 $d|f(b)-f(c)$。

例 1.1.5 常用的形式是：若 $b=qd+c$，那么，对于任何整系数多项式 $f(x)$ 而言，$d|f(b)$ 的充要条件是 $d|f(c)$。因此可以化简判断过程，亦即减少判断过程的工作量。

【例 1.1.6】 设 $f(x)=3x^5+x+6$，试判断 7 能否整除 $f(10^{100})$。

解 因为

$$10^1=10=7\cdot 1+3,\ 10^2=100=7\cdot 14+2$$

$$10^3=1000=7\cdot 142+6,\ 10^4=10\,000=7\cdot 1428+4$$

$$10^5=100\ 000=7\cdot 14\ 285+5,\ 10^6=1\ 000\ 000=7\cdot 142\ 857+1$$
$$10^7=10\ 000\ 000=7\cdot 1\ 428\ 571+3,\ \cdots$$

故当 $n=6k+r$ 时，10^n 与 10^r 除以 7 的余数相同，从而知 $10^{100}=7q+4$，故由例 1.1.5 知问题转化为判断 7 能否整除 $f(4)=3\cdot 4^5+4+6=3082$。此时很容易看出答案是否定的。

1.1.2　素数

【定义 1.1.2】 设整数 $a\neq 0$，± 1，如果它除了显然约数 ± 1、$\pm a$ 外没有其他的约数，则称 a 为**素数(或质数、不可约数)**；若 $a\neq 0$，± 1，且 a 不是素数，则称 a 为**合数**。

约定：本书所说的素数一般指正整数。这是因为当 $a\neq 0$，± 1 时，a 和 $-a$ 必同时为素数或合数，故由整除的性质知对正素数成立的结论一般对负素数也成立。

【例 1.1.7】 求 30 以内的素数。

解　利用定义 1.1.2，直接逐个计算，可知 30 以内的素数有

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29$$

关于素数，有以下结论：

【定理 1.1.1】 (i) 大于 1 的最小正因数必是素数。

(ii) n 是正整数，若对所有满足 $2\leqslant p\leqslant\sqrt{n}$ 的 p 而言，有 $p\nmid n$，则 n 是素数。

证　(i) 显然。

(ii) 用反证法。若 n 为合数，设 $n=ab$，且 $1<a\leqslant b$，那么必有 $2\leqslant a\leqslant\sqrt{n}$ 且 $a\mid n$，与已知条件矛盾，故 n 必是素数。

【定理 1.1.2】 素数有无穷多。

证　用反证法。假设只有有限个素数(注意：已约定素数一定是正的)，它们是 $q_1,\cdots,q_k$。

考虑 $a=q_1q_2\cdots q_k+1$，易知 $a>2$ 且 $a\neq q_i(i=1,2,\cdots,k)$，所以 a 必是合数，从而知必存在素数 p，使得 $p\mid a$。由假设知 p 必等于某个 q_j，因而 $p=q_j$ 一定整除 $a-q_1q_2\cdots q_k=1$，但素数 $q_j\geqslant 2$，这是不可能的，矛盾。

因此，假设是错误的，即素数必有无穷多个。

设 $q_1=2$，$q_2=3$，$q_3=5$，$q_4=7$，$q_5=11$，…是全体素数按大小顺序排成的序列，以及 $Q_k=q_1q_2\cdots q_k+1$，直接计算可得

$$Q_1=3,\ Q_2=7,\ Q_3=31,\ Q_4=211,\ Q_5=2311$$
$$Q_6=59\cdot 509,\ Q_7=19\cdot 97\cdot 277,\ Q_8=347\cdot 27\ 953$$
$$Q_9=317\cdot 703\ 763,\ Q_{10}=331\cdot 571\cdot 34\ 231$$

这里前五个($Q_1\sim Q_5$)是素数，后五个($Q_6\sim Q_{10}$)是合数，但 Q_k 都有一个比 q_k 更大的素因数。

数论中目前还未解决的问题之一就是：不知道是否有无穷多个 k 使 Q_k 是素数，也不知道是否有无穷多个 k 使 Q_k 是合数。

定理 1.1.1(ii)的一个应用就是可以减少在素数判断时的运算量，提高判断效率。因为

判断一个正整数 n 的素性(即判断 n 是否为素数)的最简单、直观的方法之一就是穷举法。即用每个小于 n 的奇素数 q 试除 n，当每个 $q\nmid n$ 时，则说明 n 是素数。而定理 1.1.1(ii)告诉我们，此时只需要对小于等于$\sqrt{n}$的奇素数 q 进行穷举即可。

【例 1.1.8】 试判断 127 的素性。

解 因为 $11<\sqrt{127}<12$，故只需用奇素数 3、5、7、11 试除 127 即可，所以 127 为素数。

由此可得到求 1 到 n 之间素数的一种有效算法——**Eratosthenes(厄拉多塞)筛法**。

为了求出不超过正整数 n 的全部素数，只要在 1 到 n 的列表中删去 1 和不超过 n 的所有正合数，则剩下的数即为所求素数。由定理 1.1.1 知，不超过 n 的正合数 a 必至少有一个素因数 p，满足 $p\leqslant\sqrt{a}\leqslant\sqrt{n}$，故只要先求出不超过$\sqrt{n}$的全部素数 p_1，p_2，…，p_k，并依次将 1 到 n 的列表中除了 p_1，p_2，…，p_k本身以外的数中是 p_1，p_2，…，p_k各自的倍数的数全部删去，就等于删除了不超过 n 的全部正合数，然后再删去 1，剩下的正好就是不超过 n 的全部素数。

例如，欲求出不超过两位数的素数，先构造 1 到 99 间正整数的列表，估计出 $\sqrt{99}<10$，然后求出小于 10 的素数 2、3、5、7，在列表中删去 1，再从中分别删去大于 2、3、5、7 且为其倍数的数，即得全部两位数的素数。具体过程如下：

~~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~~						

由此可以看出，没有删去的数有

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

共有 25 个，它们就是不超过两位数的全部素数。若再从这 25 个数出发，重复上述过程，就可以找出不超过 97^2 的全部素数。

1.1.3　带余除法

初等数论的证明中最重要、最基本、最常用的工具就是**带余除法**(或称**带余数除法**、**除法算法**、**欧几里得除法**)。

【定理 1.1.3】 设 a、b 是两个给定的整数，$b\neq0$，则一定存在唯一的一对整数 q 与 r，满足

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