现代数学基础

34 数论基础

■ 潘承洞 著

□ 展 涛 刘建亚 校

高等教育出版社
HIGHER EDUCATION PRESS

现代数学基础

34 数论基础

■ 潘承洞 著

□ 展 涛 刘建亚 校

高等教育出版社·北京
HIGHER EDUCATION PRESS BEIJING

内容简介

本书由潘承洞先生生前所写的《数论基础》讲义编辑整理而成。全书秉承了潘先生著作的一贯风格，内容由浅入深、循序渐进，既精选紧凑，又全面深刻，同时附有大量的习题。本书内容独具一格，富有启发性，能够引导读者迅速进入数论的核心领域，了解数论最基本的思想和方法。书中定理和结论的证明简洁明快，既注重数论的技巧之美，又清晰地勾勒出数论方法的系统性。全书共分七章，内容包括：整数的可除性，数论函数，素数分布的一些初等结果，同余，二次剩余与 Gauss 互反律，指数、原根和指标，Dirichlet 特征等。

本书可供数学及相关专业的本科生、研究生和教师使用参考，也可供对数论感兴趣的数学爱好者阅读。

图书在版编目（CIP）数据

数论基础 / 潘承洞著 . -- 北京 : 高等教育出版社，2012. 12

ISBN 978-7-04-036472-9

Ⅰ. ①数… Ⅱ. ①潘… Ⅲ. ①数论 Ⅳ. ① O156

中国版本图书馆 CIP 数据核字（2012）第 276324 号

策划编辑　赵天夫　　责任编辑　赵天夫　　封面设计　赵　阳　　版式设计　马敬茹
责任校对　李大鹏　　责任印制　张泽业

出版发行　高等教育出版社
社　　址　北京市西城区德外大街4号
邮政编码　100120
印　　刷　北京佳信达欣艺术印刷有限公司
开　　本　787mm×1092mm　1/16
印　　张　12.75
字　　数　190 千字
购书热线　010 - 58581118

咨询电话　400 - 810 - 0598
网　　址　http://www.hep.edu.cn
　　http://www.hep.com.cn
网上订购　http://www.landraco.com
　　http://www.landraco.com.cn
版　　次　2012年12月第1版
印　　次　2012年12月第1次印刷
定　　价　46.00元

物 料 号　36472-00

目　录

第一章　整数的可除性 **1**

§1　整除, 带余数除法 1

§2　最大公约数, 最小公倍数 5

§3　辗转相除法 11

§4　一次不定方程 14

§5　函数 $[x], \{x\}$ 16

习题 19

第二章　数论函数 **23**

§1　数论函数举例 23

§2　Dirichlet 乘积 25

§3　可乘函数 28

§4　阶的估计 38

§5　广义 Dirichlet 乘积 44

习题 51

第三章 素数分布的一些初等结果 55

§1 函数 $\pi(x)$ 55

§2 Chebyshev 定理 58

§3 函数 $\omega(n)$ 与 $\Omega(n)$ 68

§4 Bertrand 假设 72

§5 函数 $M(x)$ 76

§6 函数 $L(x)$ 81

习题 82

第四章 同余 84

§1 概念及基本性质 84

§2 剩余类及剩余系 88

§3 同余方程的一般概念, 一次同余方程 95

§4 孙子定理 101

§5 多项式的 (恒等) 同余 110

§6 模 p 的高次同余方程 113

习题 118

第五章 二次剩余与 Gauss 互反律 122

§1 二次剩余 122

§2 Legendre 符号 124

§3 Jacobi 符号 134

习题 137

第六章 指数、原根和指标 140

§1 指数和原根 140

§2　原根存在定理. 148
§3　模 p^α $(p \geqslant 2)$ 简化系的改造 151
§4　指标与指标组. 155
§5　二项同余方程. 160
习题 164

第七章　Dirichlet 特征. 167
§1　模为素数幂的特征的定义及其性质 167
§2　任意模的特征的定义及其性质 175
§3　特征和 183

校后记　. 190

第一章　整数的可除性

§1　整除，带余数除法

以 $a, b, c, q, r, \cdots$ 表示整数.

定义 1　设 a, b 为整数, $b \neq 0$, 若存在整数 c, 使 $a = bc$, 则称 b 可整除 a, 记作 $b|a$. 不然, 就称 b 不可整除 a, 记作 $b \nmid a$. 当 b 可整除 a 时, 称 b 为 a 的除数 (或因数, 约数), a 是 b 的倍数, 以及 c 是 b 除 a 所得的商.

整除的基本性质:

1) $b \neq 0$, 若 $b|a$, 则其商 c 是唯一的.

设 $a = bc_1, a = bc_2$, 则 $bc_1 = bc_2, b(c_1 - c_2) = 0$. 因为 $b \neq 0$, 所以 $c_1 = c_2$.

2) $b|a, a|e$, 则 $b|e$.

3) $b \neq 0$ 的所有倍数为 $0, \pm b, \pm 2b, \pm 3b, \cdots$.

4) $a \neq 0$, 若 $b|a$, 则 $|b| \leqslant |a|$, 等号当且仅当 $b = \pm a$ 时成立. $a\,(\neq 0)$ 的除数只有有限个, a 和 $-a$ 的除数相同. $\pm 1, \pm a$ 是 a 的显然除数. $b|a$,

若 $1<|b|<|a|$, 则称 b 为 a 的真除数.

5) 若 $b|a_1, b|a_2, m_1, m_2$ 为任意整数, 则 $b|(m_1a_1+m_2a_2)$.

定义 2 一个大于 1 的正整数, 如果除了显然除数外, 不存在其他的除数 (即无真除数), 则称为素数. 以 $p, p', p_1, p_2, \cdots$ 表示. 而有真除数的整数称为合数.

由上定义看出全体正整数 (自然数) 分为 1、素数、合数这三类数.

定理 1 任一整数 $a(\neq 0, \neq 1)$ 除 1 以外的最小正除数 d 为素数. 若 a 不是素数, 则必有 $d\leqslant\sqrt{|a|}$.

证 a 的正除数只有有限个, 所以除 1 外必有一最小的, 设为 d. 若 d 不是素数, 则必有它的真除数 d_1, 满足 $d>d_1>1$, 这和 d 为最小矛盾, 所以 d 必为素数. 设 $a=dq$. $|a|\geqslant d^2$, 所以 $d\leqslant\sqrt{|a|}$. □

定理 1 的一个重要应用是: 为了判断一个整数 $a>1$ 是否为合数, 只要用 $\leqslant\sqrt{a}$ 的素数去试除. 例如判断 103 是否为合数, 只要用 $2, 3, 5, 7$ 等去试除.

定理 2 素数有无穷多个.

证 用反证法. 设 $p_1, p_2, \cdots, p_s$ 为所有素数, 令 $n=p_1p_2\cdots p_s+1$. 设 d 为 n 的 >1 的最小正除数, 由定理 1 知 d 必为素数. 但 $d\neq p_i, i=1, 2, \cdots, s$. 因为若 $d=p_i$ 则由 $d|n, d|p_1p_2\cdots p_s$ 推出 $d|(n-p_1p_2\cdots p_s)$, 所以 $d|1$, 矛盾, 定理得证. □

定理 3 设正整数 $n>1$, 则 $n=p_1p_2\cdots p_s$, $p_1\leqslant p_2\leqslant\cdots\leqslant p_s$.

证 若 n 为素数, 则定理成立. 若 n 为合数, 则其大于 1 的最小正除数必为素数, 记为 $p_1, n=p_1n_1$, 且 n_1 的任一大于 1 的最小正除数 $\geqslant p_1$. 若 n_1 为素数, 则令 $p_2=n_1$, 定理得证. 若 n_1 不是素数, 再这样做下去, 设 n_1 的大于 1 的最小正除数为 $p_2\geqslant p_1$, 则 $n=p_1p_2n_2$. 因为 $p_1\geqslant 2, p_2\geqslant 2$, 所以这样做下去, 必在有限步内结束. 证毕. □

定理 4 (带余数除法) 设 $a, b > 0$ 为整数, 则存在唯一的一对 q 及 r, 使

$$a = qb + r, \quad 0 \leqslant r < b. \tag{1}$$

当 $r = 0$ 时, 即是 b 可整除 a.

证 作整数序列

$$\cdots, -3b, -2b, -b, 0, b, 2b, 3b, \cdots, \tag{2}$$

则 a 必在上述序列的某两项之间, 即存在一个整数 q 使得

$$qb \leqslant a < (q+1)b$$

成立. 令 $r = a - qb$, 则有 $0 \leqslant r < b$.

下面来证明唯一性. 设 r_1, q_1 是满足 (1) 的两个整数, 则

$$a = q_1 b + r_1, \quad 0 \leqslant r_1 < b. \tag{3}$$

由 (1) 及 (3) 得到

$$bq_1 + r_1 = bq + r,$$

所以

$$b(q_1 - q) = r - r_1,$$

故

$$b|q - q_1| = |r - r_1|.$$

由于 r 及 r_1 都是小于 b 的正数, 所以上式右边是小于 b 的. 如果 $q \neq q_1$, 则上式左边 $\geqslant b$, 这是不可能的. 因此必有 $q = q_1$, 从而 $r = r_1$, 得证. □

这个十分简单的定理是整个初等数论的基础. 由带余数除法可证明

定理 5 (算术基本引理) 设 $p|ab$, 且 $p \nmid a$, 则必 $p|b$.

证 不妨设 $a>0, b>0$, 考虑序列

$$a, 2a, 3a, \cdots, ka, \cdots,$$

则其中必有一些 k 使 $p|ka$, 例如 $k=p, 2p, \cdots$. 设 k_0 是使 $p|ak$ 中的最小正整数. 显然, $1<k_0 \leqslant p$, 现要证明必有 $k_0=p$. 用反证法. 若 $1<k_0<p$, 则由带余数除法得到

$$p=qk_0+r, \quad 1 \leqslant r < k_0$$

(因为 p 为素数, 所以 $r \neq 0$). 由此得到 $p|ar$. 这和 k_0 为最小矛盾, 所以必有 $k_0=p$. 下面来证明 $p|b$.

若不然, $p \nmid b$, 则由带余数除法知

$$b=qp+r \quad (0<r<p),$$

由此推出 $p|ar$, 这和 $k_0=p$ 为最小矛盾, 定理得证. □

推论 1 若 $p|a_1a_2\cdots a_s$, 则 p 至少能整除某一个 a_i.

定理 6 (算术基本定理) 设 $n>1$, 则 n 可分解为素数的乘积

$$n=p_1p_2\cdots p_s.$$

不计这些素数的次序, 则分解式是唯一的, 即

$$n=p_1^{l_1}p_2^{l_2}\cdots p_r^{l_r}, \quad p_1<p_2<\cdots<p_r, \tag{4}$$

其中 $l_i \geqslant 1, p_i (1 \leqslant i \leqslant r)$ 均由 n 所唯一决定.

证 由定理 3 知, $n>1$ 可分解为素数乘积

$$n=p_1p_2\cdots p_s, \quad p_1 \leqslant p_2 \leqslant \cdots \leqslant p_s.$$

若有另一分解式

$$n=q_1q_2\cdots q_t, \quad q_1 \leqslant q_2 \leqslant \cdots \leqslant q_t,$$

p_i, q_j 均为素数, 由于 $p_1|q_1q_2\cdots q_t$, 从推论 1 知 p_1 一定能整除某一 q_{j_0}, 所以必有 $p_1 = q_{j_0}$. 同样 $q_1|p_{i_0}$. 所以必有 $q_1 = p_{i_0}$, 从而推出 $p_1 = q_1$.

这样, 依次可证明 $p_2 = q_2, \cdots, p_s = q_s, s = t$. 把相同素数写成方幂即得 (4). □

推论 2 n 的所有正除数 $d = p_1^{i_1}p_2^{i_2}\cdots p_r^{i_r}, 0 \leqslant i_j \leqslant l_j, 1 \leqslant j \leqslant r$.

(4) 叫做 n 的标准分解式. 例如 108 的标准分解式为

$$108 = 2^2 3^3.$$

定理 6 只是一个非构造性定理. 把一个已知数分解成素因数的乘积问题是数学难题之一, 至今还没有一个实用的分解法.

§2 最大公约数, 最小公倍数

定义 3 设 $a_1, a_2, \cdots, a_k$ 是不全为零的整数. 若整数 d 是每一个 $a_i\,(1 \leqslant i \leqslant k)$ 的因数, 则 d 称为 $a_1, a_2, \cdots, a_k$ 的公因数 ($|d| \leqslant \min\limits_{a_i \neq 0}(|a_i|)$). $a_1, a_2, \cdots, a_k$ 的公因数中的最大的称为最大公因数 (或最大公约数), 记作 $(a_1, a_2, \cdots, a_k)$. 若 $(a_1, a_2, \cdots, a_k) = 1$, 则称 $a_1, a_2, \cdots, a_k$ 互素 (互质). 若其中任意两个 $a_i, a_j\,(i \neq j)$ 是互素的, 则称 $a_1, a_2, \cdots, a_k$ 是两两互素的.

定义 4 设 $b_1, b_2, \cdots, b_k$ 均不为零. 若整数 d 是每一个 $b_i\,(1 \leqslant i \leqslant k)$ 的倍数, 则 d 称为 $b_1, b_2, \cdots, b_k$ 的公倍数 ($|d| \geqslant \max\limits_i(|b_i|)$). $b_1, b_2, \cdots, b_k$ 的正的公倍数中的最小的称为最小公倍数, 记作 $[b_1, b_2, \cdots, b_k]$.

由于 a, $-a$ 的因数和倍数均相同, 所以在讨论最大公约数及最小公倍数时为了免去区别正负整数的麻烦, 可以只讨论 a_i, b_i 均大于零的情形, 亦即我们有

$$\begin{aligned}(a_1, a_2, \cdots, a_k) &= (|a_1|, |a_2|, \cdots, |a_k|),\\ [b_1, b_2, \cdots, b_k] &= [|b_1|, |b_2|, \cdots, |b_k|].\end{aligned} \tag{5}$$

由最大公约数及最小公倍数定义可得到

$$\begin{aligned} a_1|a_2, \quad &\text{则 } (a_1,a_2)=|a_1|, \quad a_1\neq 0; \\ b_1|b_2, \quad &\text{则 } [b_1,b_2]=|b_2|, \quad b_2\neq 0. \end{aligned} \tag{6}$$

定理 7 $b_1,b_2,\cdots,b_k$ 的任一公倍数, 必为其最小公倍数的倍数.

证 用反证法. 设 d 为最小公倍数, b 为任一公倍数. 若 $d\nmid b$, 则由带余数除法得到

$$b=qd+r, \quad 0<r<d.$$

然而 $r=b-qd$ 亦为 $b_1,\cdots,b_k$ 的公倍数, 但 $r<d$, 这与 d 为最小公倍数矛盾, 故必有 $d|b$. □

由此可得到下面的

推论 3

$$[[b_1,b_2,\cdots,b_i],[b_{i+1},\cdots,b_k]]=[b_1,\cdots,b_i,b_{i+1},\cdots,b_k]. \tag{7}$$

证

$$[b_1,b_2,\cdots,b_i]|[b_1,b_2,\cdots,b_k],$$
$$[b_{i+1},\cdots,b_k]|[b_1,b_2,\cdots,b_k].$$

由定理 7 知

$$[[b_1,\cdots,b_i],[b_{i+1},\cdots,b_k]]|[b_1,b_2,\cdots,b_k]. \tag{8}$$

另一方面知, 对任一 $1\leqslant l\leqslant k$, 我们有

$$b_l|[b_1,\cdots,b_i], \quad 1\leqslant l\leqslant i,$$
$$b_l|[b_{i+1},\cdots,b_k], \quad i<l\leqslant k,$$

所以对 $1\leqslant l\leqslant k$, 恒有

$$b_l|[[b_1,\cdots,b_i],[b_{i+1},\cdots,b_k]],$$

由定理 7 知

$$[b_1,\cdots,b_k]|[[b_1,\cdots,b_i],[b_{i+1},\cdots,b_k]]. \tag{9}$$

由 (8) 及 (9) 即得 (7). □

由推论 3 知求多个数的最小公倍数可化成求两个数的最小公倍数.

定理 8 $a_1,a_2,\cdots,a_k$ 的任一公因数, 一定是它们的最大公约数的因数.

证 用反证法. 设 d 为最大公约数, d_1 为任一公因数. 若 $d_1\nmid d$, 则 $[d_1,d]>d$. 但另一方面有 $d_1|a_i\,(1\leqslant i\leqslant k), d|a_i\,(1\leqslant i\leqslant k)$, 所以由定理 7 知 $[d_1,d]|a_i\,(1\leqslant i\leqslant k)$, 但这与 d 为最大公约数矛盾. □

推论 4

$$(a_1,a_2,\cdots,a_k)=((a_1,\cdots,a_i),(a_{i+1},\cdots,a_k)). \tag{10}$$

读者可自行证明之. 由此求多个数的最大公约数, 可化成求两个数的最大公约数.

定理 9 设 $m>0$, 则 $[mb_1,mb_2]=m[b_1,b_2]$.

证 因为 $m[b_1,b_2]$ 是 mb_1,mb_2 的公倍数, 所以

$$[mb_1,mb_2]|m[b_1,b_2]. \tag{11}$$

另一方面, 因为 $m|[mb_1,mb_2]$, 故可设 $[mb_1,mb_2]=md$, 这样 $mb_1|md$, $mb_2|md$, 由此推出 $b_1|d, b_2|d$, 所以 $[b_1,b_2]|d$. 由此得到

$$m[b_1,b_2]|[mb_1,mb_2], \tag{12}$$

所以必有

$$[mb_1,mb_2]=m[b_1,b_2]. \qquad \square$$

推论 5 若 $d|b_1, d|b_2$, 则

$$\left[\frac{b_1}{d}, \frac{b_2}{d}\right] = \frac{1}{d}[b_1, b_2].$$

定理 10 设 $m > 0$, 则

$$(ma_1, ma_2) = m(a_1, a_2).$$

证 由于

$$m(a_1, a_2)|ma_1, \quad m(a_1, a_2)|ma_2,$$

所以

$$m(a_1, a_2)|(ma_1, ma_2). \tag{13}$$

另一方面, 设

$$(ma_1, ma_2) = md,$$

则 $d|a_1, d|a_2$, 故 $d|(a_1, a_2)$, 所以

$$(ma_1, ma_2)|m(a_1, a_2). \tag{14}$$

由 (13), (14) 定理得证. □

推论 6 若 $d|a_1, d|a_2$, 则

$$\left(\frac{a_1}{d}, \frac{a_2}{d}\right) = \frac{1}{d}(a_1, a_2).$$

由上面的讨论知, 求最大公约数和最小公倍数时可把它们的公约数提出来, 这样只要讨论互素的情形.

定理 11 设 $a > 0, b > 0$, 则

$$(a, b)[a, b] = ab.$$

证 由于 $a|ab, b|ab$, 所以 $[a, b]|ab$, 故可设

$$ab = [a, b]m. \tag{15}$$

上式可写成

$$a=\frac{[a,b]}{b}m,\quad b=\frac{[a,b]}{a}m,$$

亦即

$$m|a,\quad m|b,$$

所以

$$m|(a,b),$$

因此 (15) 式可写成

$$ab=[a,b]\frac{(a,b)}{k}. \tag{16}$$

另一方面, 显有

$$ab=(a,b)M, \tag{17}$$

上式可写成

$$\frac{a}{(a,b)}b=M,\quad \frac{b}{(a,b)}a=M.$$

故 $a|M,b|M$, 所以 $[a,b]|M$.

因此 (17) 式可写成

$$ab=(a,b)[a,b]l. \tag{18}$$

由 (16) 及 (18) 式得到 $k=l=1$. □

利用算术基本定理亦可给出定理的另一个证明.

证 设

$$\begin{aligned}a&=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s},\quad \alpha_i\geqslant 0\quad (1\leqslant i\leqslant s),\\ b&=p_1^{\beta_1}p_2^{\beta_2}\cdots p_s^{\beta_s},\quad \beta_i\geqslant 0\quad (1\leqslant i\leqslant s),\end{aligned}$$

则

$$\begin{aligned}(a,b)&=p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_s^{\gamma_s},\quad \gamma_i=\min(\alpha_i,\beta_i)\quad (1\leqslant i\leqslant s),\\ [a,b]&=p_1^{\delta_1}p_2^{\delta_2}\cdots p_s^{\delta_s},\quad \delta_i=\max(\alpha_i,\beta_i)\quad (1\leqslant i\leqslant s).\end{aligned}$$

对于任意整数 c, d 显然有

$$c + d = \max(c, d) + \min(c, d),$$

所以我们得到

$$(a, b)[a, b] = ab. \qquad \square$$

定理 11 表明我们只要求出最大公约数就行了.

下面来证明最大公约数的两个基本性质.

定理 12 *若 a, b, c 不全为零, 且 $a = qb + c$, 则 $(a, b) = (b, c)$.*

证明留给读者.

设 a, b 不全为零, 考虑二元一次线性型 $ax + by$, 显然对任意 x, y, 一定有 $(a, b)|(ax + by)$. 下面我们要证明

定理 13 *设 a, b 不全为零, x_0, y_0 所对应的 $ax_0 + by_0$ 是使 $ax + by$ 能取到的最小正数, 则 $(a, b) = ax_0 + by_0$.*

证 我们只要证明

$$(ax_0 + by_0)|(a, b).$$

设

$$a = q_1(ax_0 + by_0) + r_1, \quad 0 \leqslant r_1 < ax_0 + by_0,$$
$$b = q_2(ax_0 + by_0) + r_2, \quad 0 \leqslant r_2 < ax_0 + by_0.$$

显然, r_1, r_2 均为 $ax + by$ 形式的数, 若 r_1 (或 r_2) $\neq 0$, 则这和 $ax_0 + by_0$ 为最小正数矛盾. 定理得证. $\square$

推论 7 *当 $(a, b) = 1$ 时, 必有 x_0, y_0 存在, 使得 $ax_0 + by_0 = 1$, 反之亦成立.*

定理 13 只是一个 "存在性" 的证明, 没有具体给出最大公约数的求法, 而是把 (a, b) 转化成另一形式 —— 二元一次线性型的最小值问

题, 但这种表达式是有用的, 它要比 (a,b) 的定义容易处理. 另外, 显然 x_0, y_0 不是唯一的, 因为 $x_0 - kb, y_0 - ka$ 也都适合要求.

定理 14 设 $(a,c)=1$, 则 $(ab,c)=(b,c)$.

证 令 $(b,c)=d$, 则 $b=b_1d, c=c_1d, (b_1,c_1)=1$,

$$(ab,c)=(ab_1d,c_1d)=d(ab_1,c_1).$$

所以只要证明 $(ab_1,c_1)=1$ 就行.

若 $(ab_1,c_1)>1$, 则必存在 p, 使得

$$p|ab_1, \quad p|c_1.$$

但由定理 5 知, 若 $p|ab_1$, 则必有 $p|a$ 或 $p|b_1$. 现在 $(a,c_1)=(b_1,c_1)=1$, 所以不可能有

$$p|a, \quad p|c_1 \quad 或 \quad p|b_1, \quad p|c_1$$

成立. 定理得证. □

推论 8 设 $(a,b)=1$, 则

$$(ab,d)=(a,d)(b,d). \tag{19}$$

定理 15 设 $(a,c)=1, c|ab$, 则必有 $c|b$.

证 因为 $(ab,c)=(b,c)=c$, 此即 $c|b$. □

§3 辗转相除法

本节要给出一种直接求出最大公约数 (a,b) 的方法, 它是反复应用带余数除法, 通常称之为辗转相除法. 在有限步后求出最大公约数 (a,b). 这种方法不但有应用价值, 且有理论价值, 用它可以来证明最大公约数的基本性质, 这种方法称为构造性方法.