信息安全数学基础

课程目标与内容

使学生掌握信息安全数学基础和理论方法，分为三部分。

第一部分为数论，包括整除、数论函数、同余、同余方程、二次同余方程、原根与指标；

第二部分为代数系统，包括代数系统和群、环和域、有限域；

第三部分为信息安全的实用算法，包括素性检验、整数分解和离散对数。

教材

使用教材：［1］杨波. 网络空间安全数学基础. 北京:清华大学出版社, 2020.

参考教材：

［1］陈恭亮. 信息安全数学基础第二版. 北京：清华大学出版社, 2014.

［2］潘承洞，潘承彪. 《初等数论》第三版，北京：北京大学出版社，2013.

［3］闵嗣鹤，严士健. 《初等数论》第四版，北京：高等教育出版社，2020.

［4］韩士安，林磊，杜荣. 《近世代数》，北京：科学出版社，2023.

［5］张禾瑞. 《近世代数基础》（修订本），北京：高等教育出版社，1978.

第一章　整除

1.1整数的概念、素数与合数

1.1整除的概念、素数与合数

数论讨论的对象是全体整数，下面以Z表示全体整数$\{\ldots,-2,-1,0,1,2,\ldots\}$构成的集合。$N$表示自然数集合。

定义1.1 设 $a,b\in Z$，$a\neq 0$，如果存在 $q\in Z$，使得$b=aq$则称 a整除 b（或称 b被 a整除），记做 $a\mid b$。这时称 b是 a的倍数，a 是 b的因数（也称因子或约数）。如果上述q 不存在，则称 a不能整除 b，记为 $a\nmid b$。

由定义1.1，0是所有非0整数的倍数。

定理1.1 （1）$a \mid b \Leftrightarrow -a \mid b \Leftrightarrow a \mid -b \Leftrightarrow |a| \,\big|\, |b|$

（2）$a \mid b$ 且 $b \mid c \Rightarrow a \mid c$

（3）$a \mid b$ 且 $a \mid c \Leftrightarrow$ 对任意的 $x, y \in Z$，有 $a \mid bx + cy$

（4）设 $m \neq 0, a \mid b \Leftrightarrow ma \mid mb$

（5）$a \mid b$ 且 $b \mid a \Rightarrow b = \pm a$

（6）设 $b \neq 0, a \mid b \Rightarrow |a| \leq |b|$

证明 （1）由 $a\mid b$，存在 $q\in Z$，使得 $b=aq$；此时 $b=(-a)(-q)$，$-b=a(-q)$，$|b|=|a|\cdot|q|$。

（2）由 $a\mid b$ 且 $b\mid c$，存在 $q_1,q_2\in Z$，使得 $b=aq_1,c=bq_2,$

（3）“$\Rightarrow$” 由 $a\mid b$ 且 $b\mid c$，存在 $q_1,q_2\in Z$，使得 $b=aq_1,c=aq_2$。则对任意 $x,y\in Z$，$bx+cy=a(q_1x+q_2y)$。

“$\Rightarrow$” 取 $x=1,y=0$，则得 $a\mid b$；取 $x=0,y=1$，则得 $a\mid b$。

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

（5）由 $b = aq_1, a = bq_2$ ，得 $a = a(q_1q_2), q_1q_2 = 1$,
所以 $q_1 = \pm 1, q_2 = \pm 1$ 。

（6）当 $b \neq 0$ 时，由 $b = aq$ ，得 $|b| = |a||q|$ 且 $|q| \geq 1$,
所以 $|b| \geq |a|$ 。

证毕。

例1.1 已知$3|n$且$7|n$，证明$21|n$

证明 由$3|n$，存在$m\in Z$，使得$n=3m$，所以$7|3m$。又由$7|7m$，所以$7|(7m-2\cdot 3m)=m$，即$m=7q,q\in Z$，所以$n=21q$，$21|n$。

例1.2 设$a=2t-1, a|2n$，证明$a|n$。

证明 由$a|2n$得$a|2tn$，$2tn=(a+1)n=an+n$。再由$a|2tn$及$a|an$得$a|2tn-an=n$。

对于任一非0整数b，± 1和$\pm b$是它的因数，称为b的显然因数。其他因数（如果存在）称为b的非显然因数或真因数。

定理1.2 对于任一$b\in Z$，$b\neq 0$，设$d_1,\cdots,d_k$是它的全体因数，则$\frac{b}{d_1},\frac{b}{d_2},\cdots,\frac{b}{d_k}$也是它的全体因数。换句话说，当$d$遍历$b$的全体因数时，$\frac{b}{d}$也遍历$b$的全体因数。

证明 显然$\frac{b}{d_1},\frac{b}{d_2},\cdots,\frac{b}{d_k}$都是整数，由$b=d_i\cdot\frac{b}{d_i}$知$\frac{b}{d_i}$都是$b$的因子$(i=1,\cdots,k)$，且当$d_i\neq d_j$时，$\frac{b}{d_i}\neq\frac{b}{d_j}$，所以$\frac{b}{d_1},\frac{b}{d_2},\cdots,\frac{b}{d_k}$也是$b$的两两不同的因数。 证毕。

定义1.2 设 $p\in Z, p\neq 0,\pm 1$，如果 p 除了因数 $\pm 1,\pm p$外，没有其他因数，则称 p 为素数（或质数），否则称为合数。

当$p\neq 0,\pm 1$时，p和$-p$同为素数或合数，所以以后没有特别说明的话，素数总指正的。

定理1.3

（1）若$d>1$，p是素数且$d\mid p$，则必有 $d=p$；

（2）若n是合数，则必存在素数 p，使得$p\mid n$；

（3）满足（2）的最小 p 一定满足$p\leq\sqrt{n}$。

证明：（1）由 $d\mid p$，存在 $q\in Z$，使得 $q>1$。若 $q>1$，则 p 为合数，矛盾。所以 $q=1$，因此 $p=d$。

（2）n 是合数，则必有 $p\in Z$，使得 $p\mid n$。如果 p 是素数，则结论得证。如果 p 不是素数，则必有因子 $q\mid p$。由定理1.1，$q\mid n$，对于 q 继续上述过程。

（3） 对于满足 $p\mid n$ 的最小的 p，一定存在 $q\in Z$，使得 $n=pq$，其中 $p\le q<n$，所以 $p^2<n, p\le\sqrt{n}$。 证毕。

定理1.4 设 $n\in Z, n\geq 2$，那么 n 一定能表示为素数的乘积。

证明 若 $n=2$，n 已经是素数，结论得证。设当 $n-1$ 时，结论成立。当 n 时，若 n 是素数，则结论成立。若 n 为合数，则必有 $n_1, n_2\in Z, 2\leq n_1, n_2<n$，使得 $n=n_1n_2$，由假设 n_1, n_2 都可表示为素数的乘积 $n_1=p_{11}p_{12}\cdots p_{1s}, n_2=p_{21}p_{22}\cdots p_{2t}$，

$n=n_1n_2=p_{11}p_{12}\cdots p_{1s}p_{21}p_{22}\cdots p_{2t}$。

证毕。

定理1.5　设 $n\in N$，如果对满足 $p\le\sqrt{n}$ 的所有素数 p，都有 $p\nmid n$，则 n 一定是素数。

证明　假定 n 是合数，则由定理1.3的(2)(3)，n 一定存在一个素因子 p，满足 $p\le\sqrt{n}$，$p\mid n$，矛盾。（（2）逆否命题）

证毕。

设基于定理1.5，要找不大于n的所有素数，先将2到n之间的整数都列出，从中删除小于等于$\sqrt{n}$的所有素数$2,3,5,7,\cdots,p_k$（设满足$p \le \sqrt{n}$的素数有k个）的倍数，余下的整数就是所要求的所有素数。这个方法称为爱拉托色尼(Eratosthenes)筛法。

例1.3 找出100以内的所有素数。

解 因为$\sqrt{100}=10$，小于10的素数有2, 3, 5, 7。删去2到100之间的整数中2的倍数（保留2）得：

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~~

删去3的倍数（保留3）得：

2	3	5	7	~~9~~
11	13	~~15~~	17	19
~~21~~	23	25	~~27~~	29
31	~~33~~	35	37	~~39~~
41	43	~~45~~	47	49
~~51~~	53	55	~~57~~	59
61	~~63~~	65	67	~~69~~
71	73	~~75~~	77	79
~~81~~	83	85	~~87~~	89
91	~~93~~	95	97	~~99~~

再分别删去5的倍数（以“—”表示，保留5）和7的倍数（以“=”表示，保留7）得：

2	3	5	7		
11	13		17	19	
	23	~~25~~		29	
31		~~35~~	37		
	41	43		47	~~49~~
		53	~~55~~		59
61		~~65~~	67		
	71	73		~~77~~	79
		83	~~85~~		89
~~91~~		~~95~~	97		

此时余下的数是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共**25**个数，就是不超过100的全部素数。从这25个数出发，又可以找出不超过1002 = 10000的全部素数。

在小于100的全体素数中，小于20的有8个，80到100之内的只有3个，所以素数的分布越来越稀。会不会到某个数以后就不存在素数，即素数的个数是有限的？答案是否定的，欧几里得用反证法正明了素数有无穷多个，开创了人类历史上反证法的先河。

定理1.6 素数有无穷多个。

证明 反证法：假设只有有限个素数，设为 $p_1, p_2, \cdots, p_k$。令 $n = p_1 p_2 \cdots p_k + 1$，$n > p_i$ 因而是合数，设 n 最小素因子为 p，必有 $p = p_j \in \{p_1, p_2, \cdots, p_k\}$。此时 $p \mid n - p_1 p_2 \cdots p_k = 1$，矛盾。故素数有无穷多个。 证毕。

素数既然有无穷多个，它的分布是不是有规律？是否能找到一个生成素数的公式，告诉我们第n个素数是什么？这个问题一直困扰着数学家，经过2000多年的努力，看来要解决它还需要很长一段时间。

素数的重要性犹如化学中的元素周期表对于化学的重要性一样，它在信息安全中也占有重要地位，可以说没有素数就没有信息安全。

1.2 最大公因子、最小公倍数、算数基本定理

1.2 最大公因子、最小公倍数、算数基本定理

1.2.1 带余数除法

定理2.1 设 a, b 是两个给定的整数，其中 $a>0$ ，则一定存在唯一的一对整数 q, r 使得 $b=aq+r$，其中 $0 \le r < a$。记 $q=\left\lfloor \frac{b}{a} \right\rfloor$ ，称为 b 被 a 除的不完全商。而 $a \mid b$ 的充要条件是 $r=0$。

证明 存在性： 将数轴上的所有整数按 a 的倍数划分成区间：$\cdots, -3a, -2a, -a, 0, a, 2a, 3a, \cdots$ 则 b 必落在某一区间，即存在 q，使得 $qa \le b < (q+1)a$。令 $r=b-qa$ ，这个 q, r 即满足要求。

唯一性： 假定还有 $q', r' \in Z$，满足 $b = aq' + r'$，其中 $0 \le r_1 < a$

但是$q \ne q'$且 $r \ne r'$（同时成立，否则一个不成立，另一个也一定不成立）。不妨设 $r' < r$，由 $aq + r = aq' + r'$ 得

$r - r' = a(q' - q)$，即 $r - r'$是 a 的倍数。但因 $0 \le r, r' < a, 0 < r - r' < a$ 矛盾。所以$r' = r$，进而，$q' = q$。

$a \mid b$的充要条件 $r = 0$，显然。 证毕。

推论 在定理2.1中，又设d是给定的整数，则存在唯一的q_1, r_1使得$b=q_1a+r_1$，其中$d \le r_1 < a+d$。

证明 对$b-d$及a，由定理2.1知存在唯一的q, r使得$b-d=qa+r$，其中$0 \le r < a$。取$q_1=q$，$r_1=r+d$，即得结论。 证毕。

在推论中取$d=0$，就是定理2.1，其中$0 \le r < a$，称为最小非负余数。取$d=1$，得$1 \le r_1 < a+1$，称为最小正余数。

当 a为偶数时，

取 $d=-\frac{a}{2}$ ，得 $-\frac{a}{2}\le r_1<\frac{a}{2}$ ；

取 $d=-\frac{a}{2}+1$ ，得 $-\frac{a}{2}<r_1\le\frac{a}{2}$ 。

当 a为奇数时，

取 $d=-\frac{a-1}{2}$ ，得 $-\frac{a-1}{2}\le r_1<\frac{a+1}{2}$ 。

后3种 r_1 称为绝对最小余数。在以后的模指数运算、多项式取模运算中，用绝对最小余数将使得计算简单。

例2.1 设 $a \geq 2$ 是给定的正整数，证明任一正整数n都可以唯一地表示为 $n = r_k a^k + r_{k-1} a^{k-1} + \cdots + r_1 a + r_0$，其中整数 $k \geq 0$
$0 \leq r_j < a \ (0 \leq j \leq k), r_k \neq 0$ 。

证明 当$n < a$ 时，取$r_1 = 0$，$r_0 = n$，得证。否则，对n, a 由定理2.1，存在唯一的正整数 $q_0, r_0 \ (0 < q_0, 0 \leq r_0 < a)$，使得 $n = q_0 a + r_0$，若 $q_0 < a$，则取 $r_1 = q_0$，得证。

若 $q_0 \ge a$，则由定理2. 1，存在唯一的正整数 q_1, r_1 $(0 < q_1, 0 \le r_1 < a)$，使得 $q_0 = q_1 a + r_1$，则 $n = q_0 a + r_0 = (q_1 a + r_1)a + r_0 = q_1 a^2 + r_1 a + r_0$。如此下去，必有正整数 $q_{k-1}, r_j (0 \le j \le k-1)$，满足 $0 < q_{k-1} < a$，$r_j < a\ (0 \le j \le k-1)$ 取 $r_k = q_{k-1}$，即得证。

例2.2 设 $a>2$ 是奇数，证明：

(1) 存在正整数 $d \le a-1$，使得 $a \mid 2^d-1$；

(2) 设 d_0 是满足(1)的最小 d，那么 $a \mid 2^h-1$ 的充要条件是 $d_0 \mid h$。

证明 (1) 考虑以下 a 个数：$2^0, 2^1, 2^2, \cdots, 2^{a-1}$，由 $2^0=1, 2^j(j=1,\cdots,a-1)$ 是偶数得 $a\nmid 2^j(j=0,\cdots,a-1)$。由定理2.1，存在 q_j, r_j。使得 $2^j = q_j a + r_j$，$0 < r_j < a$，即 a 个余数 $r_0, r_1, \cdots, r_{a-1}$ 只可能在 $1,2,\cdots,a-1$ 这 $a-1$ 个值中取。由鸽舍原理，必有2个相等，设为 r_i, r_k，不妨设 $0 \le i < k \le a-1$，因而 $2^k - 2^i = 2^i(2^{k-i}-1) = (q_k - q_j)a$ 所以 $a \mid 2^i(2^{k-i}-1)$，$a \mid 2^{k-i}-1$。取 $d = k-i$ 就满足要求。

(2) **充分性：** 当 $d_0 \mid h$ 时，$a \mid 2^{d_0}-1, 2^{d_0}-1 \mid 2^h-1$，所以 $a \mid 2^h-1$。

必要性： 由定理2.1，存在 q, r 使得 $h = qd_0 + r$，其中 $0 \le r < d_0$，因而$2^h-1 = 2^{qd_0+r}-2^r+2^r-1 = 2^r(2^{qd_0}-1)+(2^r-1)$ 由 $a \mid 2^h-1, a \mid 2^{qd_0}-1$，得 $a \mid 2^r-1$。由 d_0 的最小性，得 $r=0$。所以 $d_0 \mid h$。

1.2.2 最大公因子

定义2.1 设 a_1, a_2 是两个不同时为0的整数，如果 $d\,|\,a_1$ 且 $d\,|\,a_2$ ，则称 d 为 a_1, a_2 的公因子。公因子中最大的称为 a_1, a_2 的最大公因子，记为 (a_1, a_2) 。一般地，设 $a_1, \cdots, a_k$ 是 k 个不同时为0的整数，如果 $d\,|\,a_1, d\,|\,a_2, \cdots, d\,|\,a_k$ ，则称 d 为 $a_1, a_2, \cdots, a_k$ 的公因子。公因子中最大的称为最大公因子，记为 $(a_1, a_2, \cdots, a_k)$ 。若 $(a_1, a_2) = 1$, 则称 a_1, a_2 是互素的。$(a_1, \cdots, a_k) = 1$ ，则称 $a_1, \cdots, a_k$ 是互素的。

例如， $a_1=12, a_2=18$ 他们的公因子是 $\pm1,\pm2,\pm3,\pm6,(12,18)=6$，$a_1=6, a_2=10,\ a_3=-15,$ 公因子是 ±1，$(6,10,-15)=1$，即6，10，-15 是互素的。

例2.3 设 p 为素数，a 为整数，证明 $(p,a)=\begin{cases} p, & p\mid a; \\ 1, & p\nmid a. \end{cases}$

证明 设 $d=(p,a)$，则有 $d\mid p, d\mid a$。因为 p 是素数，所以 $d=1$ 或 $d=p$。若 $p\mid a$，则 p 是 p 和 a 的公因子，因而 $p\le d$。但 $d\mid p$，$d\le p$，所以 $d=p$。若 $p\nmid a$，则必有 $d=1$，否则由 $d=p$ 得 $p\mid a$，矛盾。

定理2.2 设 a,b 是2个不同时为0的整数，则存在 $x,y\in Z$，使得 $(a,b)=ax+by$。

证明 对任意 $u,v\in Z$，考虑所有形如 $au+bv$ 的整数构成的集合。选 $x,y\in Z$，使得 $m=ax+by$ 是该集合中最小的正整数。由定理2.1，存在唯一的 q,r，使得 $a=mq+r$，其中 $0\le r<m$。因而有 $r=a-mq=a-(ax+by)q=(1-qx)a+(-qy)b$ 即 r 也是 a,b 的线性组合。由 m 的最小性，$r=0$。所以，$a=mq$ $m\mid a$。类似地 $m\mid b$，即 m 是 a,b 的公因子，$m\le(a,b)$。又因 $(a,b)\mid a$，$(a,b)\mid b$，得 $(a,b)\mid m=ax+by$，$(a,b)\le m$，所以 $m=(a,b)$。 证毕。

定理2.3 设a,b是2个不同时为0的整数,$d=(a,b)$的充要条件是:

（1） $d\mid a, d\mid b$ ；

（2）若$e\mid a, e\mid b$ ，则 $e\mid d$ 。

证明 **必要性：** 条件(1)显然，下面证条件(2)，由定理2.2，存在$x,y\in Z$，使得$d=ax+by$。由$e\mid a, e\mid b$ 得 $e\mid d$。

充分性： 由(1)，d 是a,b 的公因子。由(2)，对任一$e\in Z$满足$e\mid a, e\mid b$，即e是 a,b的公因子，有 $e\mid d$ ，即 $e\le d$ ，所以d是公因子中最大的。 证毕。

定理2.3也可作为最大公因子的定义，使用起来比定义2.1更为直观，以后主要使用该定义。

定理2.4 设 a, b 是2个不同时为0的整数，a, b 互素的充要条件是存在 $x, y \in Z$，使得 $xa + yb = 1$。（贝祖等式）

证明 **必要性：**$(a, b) = 1$，由定理2.2直接得到。

充分性：设 $d = (a, b)$，则$d \mid a, d \mid b$，所以$d \mid xa + yb = 1, d = 1$

证毕。

定理2.5 设 a是非0的整数，如果$a \mid bc$且 (a,b)=1，则 $a \mid c$ 。

证明 由$(a, b) = 1$ 及定理2.2，存在$x, y \in Z$，使得$xa + yb = 1$

两边同乘c，得 $xac + ybc = c$ 。因为$a \mid xac, a \mid ybc$ ，所以 $a \mid c$。 证毕。

定理2.6　设a,b是2个不同时为0的整数，

（1）对任一正整数m, 有$(ma,mb)=m(a,b)$；

（2）设非0整数d 满足$d\mid a, d\mid b$，则$\left(\frac{a}{d},\frac{b}{d}\right)=\frac{(a,b)}{|d|}$。特别地$\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1$。

证明 （1）设 $d=(a,b),d'=(ma,mb)$ 。则由 $d\mid a,d\mid b$ 得 $md\mid ma,\ md\mid mb$，即 md 是 ma,mb 的公因子，所以 $md\mid d'$

又由 $d=(a,b)$，存在 $x,y\in Z$，使得 $xa+yb=d$，两边同时乘以 m 得 $x(ma)+y(mb)=md$。因为 $d'\mid ma,d'\mid mb$ ，所以 $d'\mid md$。因此有 $d'=md$ 。

（2）$(a,b)=\left(|d|\frac{a}{|d|},|d|\frac{b}{|d|}\right)=|d|\left(\frac{a}{|d|},\frac{b}{|d|}\right)=|d|\left(\frac{a}{d},\frac{b}{d}\right)$

所以$\left(\frac{a}{d},\frac{b}{d}\right)=\frac{(a,b)}{|d|}$。取$d=(a,b)$，则有$\left(\frac{a}{(a,b)},\frac{b}{(a,b)}\right)=1$。

证毕。

定理2.7 设 $a_1, a_2, \cdots, a_n$ 是 n 个不全为0的整数，$(a_1, a_2) = d_2$
$(d_2, a_3) = d_3$，$\cdots$，$(d_{n-1}, a_n) = d_n$ 则 $(a_1, a_2, \cdots, a_n) = d_n$ 。

证明 由 $(d_{n-1}, a_n) = d_n$ 知 $d_n \mid d_{n-1}$，$d_n \mid a_n$，但 $d_{n-1} \mid d_{n-2}$，$d_{n-1} \mid a_{n-1}$，所以 $d_n \mid d_{n-2}$，$d_n \mid a_{n-1}$。继续下去得 $d_n \mid d_2$，$d_n \mid a_3$。又由 $d_2 \mid a_1$，$d_2 \mid a_2$ 得 $d_n \mid a_2$，$d_n \mid a_1$，所以 d_n 是 $a_1, a_2, \cdots, a_n$ 的公因子。又设 d 是 $a_1, \cdots, a_n$ 的任一公因子，由 $d \mid a_1$，$d \mid a_2$ 得 $d \mid d_2$。再由 $d \mid a_3$，又得 $d \mid d_3$。继续下去得到 $d \mid d_n$，由定理2.3，d_n 是 $a_1, a_2, \cdots, a_n$ 的最大公因子。

证毕。

最大公因数的运算性质

定理1.3.11 设a, b, c是三个整数, 且$b \neq 0$, $c \neq 0$. 如果$(a, c) = 1$, 则

$$(a \cdot b, c) = (b, c).$$

证 令$d = (a \cdot b, c)$, $d' = (b, c)$. 有$d' \mid b$, $d' \mid c$. 进而$d' \mid a \cdot b$, $d' \mid c$. 再根据定理1.3.9, 得到$d' \mid d$.

反过来, 因为$(a, c) = 1$, 根据贝祖等式, 存在整数s, t 使得 $s \cdot a + t \cdot c = 1.$

两端同乘b, 得到 $$s \cdot (a \cdot b) + (t \cdot b) \cdot c = b.$$

再由 $d \mid a \cdot b$, $d \mid c$, 得到 $d \mid s \cdot (a \cdot b) + (t \cdot b) \cdot c$, 即 $d \mid b$.

同样根据定理1.3.9, 得到$d \mid d'$.

故$d = d'$. 定理成立. 证毕

定理1.3.12 设$a_1, \ldots, a_n, c$为整数. 如果$(a_i, c) = 1,\ 1 \le i \le n$. 则

$$(a_1 \cdots a_n,\ c) = 1.$$

证 对n作数学归纳法. $n = 2$时, 命题由定理1.3.11得到.
也可直接证明. 设$(a_1, c) = 1,\ (a_2, c) = 1$, 则存在整数$s_1,\ t_1$和$s_2,\ t_2$使得

$$s_1 \cdot a_1 + t_1 \cdot c = 1, \qquad s_2 \cdot a_2 + t_2 \cdot c = 1.$$

进而, $(s_1 s_2) \cdot (a_1 a_2) = (1 - t_1 \cdot c)(1 - t_2 \cdot c) = 1 - (t_1 + t_2 - t_1 t_2 c) \cdot c,$

或 $(s_1 s_2) \cdot (a_1 a_2) + (t_1 + t_2 - t_1 t_2 c) \cdot c = 1$

因此得到，$(a_1 \cdot a_2, c) = 1$

(续) **定理1.3.12** 设$a_1,\ \ldots,\ a_n,\ c$ 为整数. 如果$(a_i,c)=1,\ 1\le i\le n$. 则

$$(a_1\cdots a_n,\ c)=1.$$

证 假设$n-1$ 时, 命题成立. 即 $(a_1\cdots a_{n-1},\ c)=1.$
对于n, 根据归纳假设, 有

$$(a_1\cdots a_{n-1},\ c)=1.$$

再根据$(a_n,c)=1$ 及定理1.3.11, 得到

$$(a_1\cdots a_{n-1}a_n,\ c)=((a_1\cdots a_{n-1})a_n,\ c)=1.$$

1.2.3 最小公倍数

定义2.2 设 a_1, a_2 是2个均不为0的整数，$m \in \mathbb{Z}$，满足 $a_1 \mid m$ 且 $a_2 \mid m$，则称 m 是 a_1, a_2 的公倍数。满足上述条件的最小正 m 称为 a_1, a_2 的最小公倍数，记为 $[a_1, a_2]$。设 $a_1, \cdots, a_k$ 是 k 个均不为0的整数，$m \in \mathbb{Z}$，满足 $a_1 \mid m, \cdots, a_k \mid m$，则称 m 是 $a_1, \cdots, a_k$ 的公倍数。类似地有 $a_1, \cdots, a_k$ 的最小公倍数 $[a_1, \cdots, a_k]$。

例如 $a_1 = 2, a_2 = 3$，他们的公倍数集合为 $\{0, \pm 6, \pm 12, \cdots, \pm 6k, \cdots\}$

$[a_1, a_2] = 6$。

注：由于任何正数都不是0的倍数，故讨论整数的最小公倍数时，一概假定这些整数都不是0

定理2.8 设a,b是2个均不为0的整数，$m=[a,b]$的充要条件是：

（1）$a|m, b|m$；

（2）若 $a|M$，$b|M$，则 $m|M$。

证明 必要性： 条件(1)显然。下面证明条件(2)，由定理2.1，存在q,r使得$M=qm+r$，其中$0\le r<m$。由$a|M$，$a|m$ 得 $a|r$，类似地$b|r$。所以r是a,b的公倍数，由m的最小性知 $r=0$，所以 $M=qm$。

充分性： 显然。 证毕。

定理2.8也可以作为最小公倍数的定义，使用起来更方便。

定理2.9 设 a,b是2个互素的正整数，则 $[a,b]=a\cdot b$ 。

证明 设$m=ab$，显然 m是 a,b的公倍数。设M也是 a,b的公倍数，由 $a\mid M$ ，存在$q>0$，使得 $M=aq$ 。由 $b\mid M$ ， $b\mid aq$。因 $(a,b)=1$ ，由定理2.5得 $b\mid q$，所以存在 $q'>0$ ，使得 $q=bq'$ 。因此 $M=aq=abq'=mq'$，即 $m\mid M$ 。所以 $m=[a,b]$ 。 证毕。

定理2.10 设 a，b 是2个均不为0的正整数。

（1）对任一正整数 k，有 $[ka,kb]=k[a,b]$；

（2）$[a,b]\cdot(a,b)=ab$ 。

证明 (1) 设 $m=[a,b]$，$m'=[ka,kb]$。由 $ka\mid m'$，$kb\mid m'$，得 $a\mid\dfrac{m'}{k}$，$b\mid\dfrac{m'}{k}$，所以 $m\mid\dfrac{m'}{k}$，即 $km\mid m'$。另一方面，由 $a\mid m$，$b\mid m$，得 $ka\mid km$，$kb\mid km$，因此 $m'\mid km$。所以 $m'=km$。

(2) 由定理2.6知 $\left(\dfrac{a}{(a,b)},\dfrac{b}{(a,b)}\right)=1$，再由定理2.9得 $\left[\dfrac{a}{(a,b)},\dfrac{b}{(a,b)}\right]=\dfrac{ab}{(a,b)^2}$，两边同乘以 $(a,b)^2$ 即得。

证毕。

定理2.11 设 $a_1,\cdots,a_n \in Z$，$[a_1,a_2]=m_2$，$[m_2,a_3]=m_3$，$\cdots$ $[m_{n-1},a_n]=m_n$， 则 $[a_1,\cdots,a_n]=m_n$ 。

证明 由 $[a_1,a_2]=m_2$ 知 $a_1\mid m_2$，$a_2\mid m_2$。 由 $[m_2,a_3]=m_3$ 知 $m_2\mid m_3$，$a_3\mid m_3$， 所以 $a_1\mid m_3$，$a_2\mid m_3$，$a_3\mid m_3$。如此下去，由 $[m_{n-1},a_n]=m_n$， 知 $m_{n-1}\mid m_n$，$a_n\mid m_n$ 得 $a_1\mid m_n$，$a_2\mid m_n$ $\cdots$，$a_n\mid m_n$， 即 m_n 是 $a_1,\cdots,a_n$ 的公倍数。

又设m'是$a_1,\cdots,a_n$的任一公倍数, 则 $a_1\mid m', a_2\mid m',\cdots,a_n\mid m'$

由 $[a_1,a_2]=m_2$得 $m_2\mid m'$。又由$[m_2,a_3]=m_3$ 及 $a_3\mid m'$

得$m_3\mid m'$。如此下去，得 $m_{n-1}\mid m'$。再由 $a_n\mid m'$

得$[m_{n-1},a_n]=m_n\mid m'$。所以m_n是$a_1,\cdots,a_n$的最小公倍数。

证毕。

1.2.4 算术基本定理

定理1.4已经证明任一正整数可以分解为素数的乘积，下面将证明正整数的这种分解在不记次序的意义下是唯一的。先证明如下结论。

定理2.12 设 p 是素数，$p \mid a_1a_2$，则 $p \mid a_1$ 和 $p \mid a_2$ 至少有一个成立。一般地，若 $p \mid a_1 \cdots a_k$，则 $(i=1,\cdots,k)$ 至少有一个成立。

证明 若 $p \nmid a_1$，则由例2.3知 $(p, a_1)=1$。由定理2.5得 $p \mid a_2$。一般情况下类似地证明。 证毕。

定理2.13　（算术基本定理）设 n 是大于1的正整数，必有 $n = p_1 p_2 \cdots p_s$，其中 p_i 是素数。且在不计素因子的次序时，这个分解式是唯一的。

证明　下面仅证明唯一性，不妨设 $p_1 \le p_2 \le \cdots \le p_s$。若还有另一种解式 $n = q_1 q_2 \cdots q_r$，其中 $q_1 \le q_2 \le \cdots \le q_r$，下面证明 $r = s$ $p_j = q_j\ (1 \le j \le s)$。不妨设 $s \le r$，由定理2.12，$q_1 \mid n = p_1 \cdots p_s$，必有某个 p_j，使得 $q_1 \mid p_j$，但由于 q_1 和 p_j 都是素数，所以 $q_1 = p_j$ 同理对 p_1，必有某个 q_i，使得 $p_1 = q_i$。

由于$q_1 \le q_i = p_1 \le p_j = q_1$，所以 $p_1 = q_1$。这样由 $p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_r$ 可得到 $p_2 p_3 \cdots p_s = q_2 q_3 \cdots q_r$ 同理可得 $p_2 = q_2, \cdots, p_s = q_s$ 。若 $s < r$，则有$q_{s+1} \cdots q_r = 1$，这是不可能的。所以有$s = r$，$p_j = q_j \ (1 \le j \le s)$ 。

证毕。

合并分解式中相同的素数，即得 $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$，其中 $p_1 < p_2 < \cdots < p_s$，这个分解式称为标准分解式。

定理2. 14 设 $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$, $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$ 是正整数a,b的标准分解式，则有

（1）$a \cdot b = p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \cdots p_s^{\alpha_s+\beta_s}$；

（2）$a \mid b \Leftrightarrow \alpha_i \le \beta_i \ (1 \le i \le s)$；

（3）$(a,b) = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$，其中 $e_i = \min\{\alpha_i, \beta_i\}, 1 \le i \le s$；

（4）$[a,b] = p_1^{d_1} p_2^{d_2} \cdots p_s^{d_s}$，其中 $d_i = \max\{\alpha_i, \beta_i\}, 1 \le i \le s$；

（5）$(a,b)[a,b] = ab$。

证明

(1) 显然。

(2) “$\Leftarrow$” 由 $\alpha_i \le \beta_i$ 得 $b = aq$，其中 $q = p_1^{\beta_1-\alpha_1} p_2^{\beta_2-\alpha_2} \cdots p_s^{\beta_s-\alpha_s}$。

“$\Rightarrow$” 由 $a \mid b$，$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \mid p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s}$，若 $\alpha_1 > \beta_1$，则 $p_1^{\alpha_1-\beta_1} p_2^{\alpha_2} \ldots p_s^{\alpha_s} \mid p_2^{\beta_2} \ldots p_s^{\beta_s}$，则 $p_1 \mid p_1^{\alpha_1-\beta_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} \mid p_2^{\beta_2} \cdots p_s^{\beta_s}$。存在 $p_i\,(2 \le i \le s)$，使得 $p_1 \mid p_i$，因此 $p_1 = p_i$，矛盾。所以$\alpha_1 \le \beta_1$，类似地 $\alpha_i \le \beta_i\,(2 \le i \le s)$。

(3) 设 $c = p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s}$，由 $e_i \le \alpha_i\ (1 \le i \le s)$ 得 $c \mid a$，同理

$c \mid b$。又设 $c' = p_1^{e_1'} p_2^{e_2'} \dots p_s^{e_s'}$，满足 $c' \mid a$，$c' \mid b$。由(2)

得 $e_i' \le \alpha_i$，$e_i' \le \beta_i\ (1 \le i \le s)$，因此 $e_i' \le \min\{\alpha_i, \beta_i\} = e_i$，

得 $c \mid c'$。所以 $c = (a, b)$。

（4）设 $d = p_1^{d_1} p_2^{d_2} \cdots p_s^{d_s}$，由 $\alpha_i \le d_i \ (1 \le i \le s)$，得 $a \mid d$ 同理 $b \mid d$。又设 $d' = p_1^{d_1'} p_2^{d_2'} \cdots p_s^{d_s'}$，满足 $a \mid d'$，$b \mid d'$，由(2)得 $\alpha_i \le d_i'$，$\beta_i \le d_i' \ (1 \le i \le s)$，因此 $d_i = \max\{\alpha_i, \beta_i\} \le d_i' (1 \le i \le s)$，由此 $d \mid d'$。所以 $d = [a, b]$

（5）由(3)(4)得 $(a, b)[a, b] = p_1^{e_1+d_1} p_2^{e_2+d_2} \cdots p_s^{e_s+d_s}$，而 $e_i + d_i = \max\{\alpha_i, \beta_i\} + \min\{\alpha_i, \beta_i\} = \alpha_i + \beta_i$，所以 $(a, b)[a, b] = p_1^{\alpha_1+\beta_1} p_2^{\alpha_2+\beta_2} \cdots p_s^{\alpha_s+\beta_s} = a \cdot b$。

证毕。

例如 $45=2^0\cdot3^2\cdot5, 100=2^2\cdot3^0\cdot5^2$，$(45,100)=2^0\cdot3^0\cdot5^1=5$，

$[45,100]=2^2\cdot3^2\cdot5^2=900$ 。

利用整数的标准分解式可求整数的最大公因子和最小公倍数。然而这种方法仅限于整数比较小的情况，对于大整数来说求标准分解式本身就是一个困难问题。一般情况下，求整数的最大公因子可用下节介绍的Euclid算法。

定理2.15 设 $a,b\in N$，则存在 $a'\mid a$，$b'\mid b$，使得

$$a'\cdot b'=[a,b],\ (a',b')=1。$$

证明 设 $a=p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，$b=p_1^{\beta_1}\cdots p_s^{\beta_s}$，其中 $\alpha_i\ge\beta_i\ge 0\,(i=1,\cdots,t)$，$\beta_i>\alpha_i\,(i=t+1,\cdots,s)$，则取 $a'=p_1^{\alpha_1}\cdots p_t^{\alpha_t}$，$b'=p_{t+1}^{\alpha_{t+1}}\cdots p_s^{\alpha_s}$ 即为所求。

证毕。

1.3 Euclid算法

1.3.1 Euclid定理

定理3.1 对任意 $a,b,q\in Z$ ，有 $(a,b)=(a,b-qa)$。

证明 设 $d\mid a$ ，$d\mid b$ ，则 $d\mid b-qa$ ，即 a,b 的公因子也是 a，$b-qa$ 的公因子。类似地设 $d'\mid a$，$d'\mid b-qa$，则 $d'\mid(b-qa)+qa=b$，即 a 和 $b-qa$ 的公因子也是 a,b 的公因子。所以得 a,b 的公因子集合和 $a,b-qa$ 的公因子集合相等，两个集合中的最大值相等。

证毕。

按定理3.1，$(a,b)=(a,b-a)$，所以求 (a,b) 时可以连续地从a,b中的大的减去小的，直到得到0，由$(a,0)=|a|$就得结果。

定理3.1是Euclid提出的最初形式，把它用在带余数除法中，得到的是Euclid算法的现代版。

设 a,b 是两个整数，$a>0$ ，在定理3.1中，将 q取为带余数除法中的 q，则得 $(a,b)=(a,r)$。

例3.1 对任意$n\in Z$，

$$(21n+4,14n+3)=\left(21n+4-(14n+3),14n+3\right)=(7n+1,14n+3)$$
$$=\left(7n+1,14n+3-2(7n+1)\right)=(7n+1,1)=1$$

例3.2 对任意$n\in Z$，$(n-1,n+1)=(n-1,2)=\begin{cases}1, & 2\mid n;\\ 2, & 2\nmid n.\end{cases}$。

例3.3 对任意$n\in Z$，$(2n-1,n-2)=(2n-1-2(n-2),n-2)=(3,n-2)$

当$n=3k$时，$(2n-1,n-2)=(2n-1-2(n-2),n-2)=(3,n-2)$。

当$n=3k+1$时，$(3,n-2)=(3,3k-2)=(3,3(k-1)+1)=(3,1)=1$。

当$n=3k+2$时，$(3,n-2)=(3,3k)=3$。

定理3.2 设$m, n, t \in Z$, $m>0$, $n>0$, 则$(t^n-1,\ t^m-1)=t^{(m,n)}-1$

证明 对$\max(n,m)$用归纳法。当$\max(n,m)=1$或$n=m$时，结论显然。否则假定$m<n$，由$(t^n-1)-t^{n-m}(t^m-1)=t^{n-m}-1$，得$(t^n-1, t^m-1)=(t^m-1, t^{n-m}-1)=t^{(m,n-m)}-1=t^{(n,m)}-1$其中第2步由归纳假设得，第3步由定理3.1得。

证毕。

推论 $t^n-1\mid t^m-1$当且仅当$n\mid m$ 。

证明 若$n\mid m$，则$\left(t^n-1,t^m-1\right)=t^{(m,n)}-1=t^n-1$，所以$t^n-1\mid t^m-1$ 反之，若$t^n-1\mid t^m-1$ ，则$\left(t^n-1,t^m-1\right)=t^n-1$ 即$t^{(m,n)}-1=t^n-1$ 。所以$(m,n)=n$，$n\mid m$ 。

证毕。

定理3.3 设m,n,q是正整数，则$(x^{q^m}-x,x^{q^n}-x)=x^{q^{(m,n)}}-x$。

证明 连续两次应用定理3.2即可证得。 证毕。

推论 设m,n,q是正整数，则$x^{q^n}-x\mid x^{q^m}-x$当且仅当$n\mid m$。

证明 若$n\mid m$，则$(m,n)=n$, $\left(x^{q^m}-x,x^{q^n}-x\right)=x^{q^{(m,n)}}-x=x^{q^n}-x$

所以$x^{q^n}-x\mid x^{q^m}-x$。

反之，若$x^{q^n}-x\mid x^{q^m}-x$，则$\left(x^{q^m}-x,\ x^{q^n}-x\right)=x^{q^n}-x$。又$\left(x^{q^m}-x,\ x^{q^n}-x\right)=x^{q^{(m,n)}}-x$，所以$x^{q^{(m,n)}}-x=x^{q^n}-x$。

$(m,n)=n$，所以$n\mid m$。

证毕。

1.3.2 广义Euclid除法

广义Euclid除法也称为辗转相除法，用于求两个正整数的最大公因子。设 a,b 是2个正整数，不妨假定 $a>b$，记 $r_{-1}=a$，$r_0=b$，反复用带余数除法，有

$$r_{-1}=q_1r_0+r_1 \qquad 0<r_1<r_0 \ ,$$

$$\cdots\cdots$$

$$r_{n-2}=q_nr_{n-1}+r_n \qquad 0<r_n<r_{n-1} \ ,$$

$$r_{n-1}=q_{n+1}r_n+r_{n+1} \qquad r_{n+1}=0 \ 。$$

因此 $r_{n+1}<r_n<r_{n-1}<\cdots<r_0=b$，所以经过有限步后必有某个 $r_{n+1}=0$ 。此时$r_n=(a,b)$，这是因为

$$(a,b)=(r_{-1},r_0)=\cdots=(r_{n-1},r_n)=(r_n,r_{n+1})=(r_n,0)=r_n \ 。$$

由上还可得：

$$r_n = r_{n-2} - q_n r_{n-1} \quad ,$$

$$r_{n-1} = r_{n-3} - q_{n-1} r_{n-2} \quad ,$$

$$\cdots\cdots$$

$$r_1 = r_{-1} - q_1 r_0 \quad 。$$

依次将后一项带入前一项，可得 r_n由 $r_{-1} = a$ ，$r_0 = b$ 的线性组合表示。

例3.4 已知$a=-1859$，$b=1573$，求(a,b)及整数s，t使得$sa+tb=(a,b)$。

解 因为，用广义Euclid除法得

$$1859=1\cdot 1573+286$$

$$1573=5\cdot 286+143$$

$$286=2\cdot 143+0$$

所以 $(a,b)=143$ 。

而 $143=1573-5\cdot 286=1573-5\cdot(1859-1\cdot 1573)=5\cdot(-1859)+6\cdot 1573$

即 $s=5, t=6$， $sa+tb=(a,b)$ 。

这种反向带入法求 s,t 时需要记下所有中间结果 r_i , q_i 。下面给出一种递推法，可直接求出 s,t，此时需要引入2个新的序列$\{s_i\},\{t_i\}$。

定理3.4 设a, b如上，在以上辗转相除法中，当$r_{n+1}=0$时，

$$s_n a + t_n b = (a,b) \qquad (3.1)$$

其中s_i，t_i按如下递推方式定义：

初值：$\begin{cases} s_{-1}=1,\ t_{-1}=0; \\ s_0=0,\ t_0=1. \end{cases}$

递推式：$\begin{cases} s_i = s_{i-2} - q_i s_{i-1} \\ t_i = t_{i-2} - q_i t_{i-1} \end{cases} \qquad (3.2)$

其中$q_i = \left\lfloor \dfrac{r_{i-2}}{r_{i-1}} \right\rfloor$。

证明 为了证明式（3.1），只须证明对每一$i=-1,0,1,\cdots,n$，

$$s_i a + t_i b = r_i \qquad (3.3)$$

成立。

用归纳法，当 $i=-1$ 时，$s_{-1}a+t_{-1}b=a=r_{-1}$，（3.3）成立。

当 $i=0$ 时，$s_0a+t_0b=b=r_0$，（3.3）成立。

设（3.3）式对所有 $i\le k-1$ 成立，则当 $i=k$ 时，

$$r_k=-q_kr_{k-1}+r_{k-2}=-q_k(s_{k-1}a+t_{k-1}b)+(s_{k-2}a+t_{k-2}b)$$
$$=(s_{k-2}-q_ks_{k-1})a+(t_{k-2}-q_kt_{k-1})b=s_ka+t_kb$$

证毕。

计算过程可列表如下：

表1-1 广义Euclid除法

j	s_{j-1}	s_j	t_{j-1}	t_j	q_{j+1}	r_j	r_{j+1}
-1	–	1	–	0	–	a	b
0	1	0	0	1	q_1	b	r_1
…							
i	s_{i-1}	s_i	t_{i-1}	t_i	q_{i+1}	r_i	r_{i+1}
…							
n	s_{n-1}	s_n	t_{n-1}	t_n	q_{n+1}	r_n	$r_{n+1}=0$

表的建立过程如下：首先将初值 $s_{-1}=1$，$t_{-1}=0$，$s_0=0$，$t_0=1$，$r_{-1}=a$，$r_0=b$ 填入。第 i 行如下建立：s_{i-1} 取上一行的 s_i，即它的右上元素，s_i 由递推式 $s_i=s_{i-2}-q_is_{i-1}$ 计算，其中 q_i 是上一行的 q_i。t_{i-1} 和 t_i 的取法类似。q_{i+1} 由上一行的 r_{i-1} 和 r_i 得 $q_{i+1}=\left\lfloor \frac{r_{i-1}}{r_i} \right\rfloor$。$r_i$ 取上一行的 r_i，即它的右上元素，r_{i+1} 由递推公式 $r_{i+1}=r_{i-1}-q_{i+1}r_i$ 得，直到 $r_{n+1}=0$ 为止。

例3.5 用递推法求例3.4

解： 计算过程如表1.2所示。

表3-2 例3.5计算过程

j	s_{j-1}	s_j	t_{j-1}	t_j	q_{j+1}	r_j	r_{j+1}
-1	—	1	—	0	—	1859	1573
0	1	0	0	1	1	1573	286
1	0	1	1	-1	5	286	143
2	1	-5	-1	6	2	143	0

得 $s=-5$，$t=6$，$(-5)\cdot 1859+6\cdot 1573=143$。或写成

$5\cdot(-1859)+6\cdot 1573=143$。