信息安全数学基础

信息安全工程大学

第1章 整数的可除性

1.1 整除

【定义1.1.1】 设$a, b \in Z$（整数集合），$b \neq 0$, 如果存在$q \in Z$, 使得$a = bq$, 则称b整除a或a可被b**整除**, 记作$b|a$, 并称a是b的**倍数**, b是a的**因数**（或约数、因子）. 否则, 称b不能整除a或a不能被b整除, 记作$b \nmid a$.

对于整除, 应注意下述的特殊情况:

① 0是任何非零整数的倍数.

② ±1是任何整数的因数.

③ 任何非零整数是其自身的倍数, 也是其自身的因数.

整除的一些基本性质

① 设$a, b \in Z$, 若 $b|a$, 则$b|-a, -b|-a$;

② $c|b, b|a$, 则$c|a$.

证: $c|b, b|a$, 故存在q_1, q_2, 使$b = cq_1, a = bq_2$, 故 $a = cq_1q_2$, 故$c|a$.

③ $c|b, c|a$, 则$c|a \pm b$.

证: $c|b, c|a$, 则存在整数n, m, 使得$b = nc, a = mc$. 故 $a \pm b = mc \pm nc = (m \pm n)c$.

整除的一些基本性质

④ 设p为素数, 若$p \mid ab$, 则$p \mid a$或$p \mid b$.

⑤ $c|b, c|a$, 则对任意整数s, t, 有$c|sa \pm tb$.

证明: $c|b, c|a$, 则存在整数n, m, 使得$b = nc, a = mc$.

则$sa \pm tb = msc + ntc = (ms + nt)c$.

该性质也描述为: $c|b, c|a$, 则c整除a和b的线性组合.

【例1.1.1】 $7|21, 7|98$, 则对任意整数$s, t, 7|21s + 98t$.

素数

【定义1.1.2】 设p是大于1的整数, 如果除了约数1和它本身外没有其它的约数, 那么, p就称为素数（或质数）. 若m是大于1的整数, 且m不是素数, 则m称为合数.

素数的一些基本性质:

① 1既不是素数也不是合数.

② p为素数, n是正整数, 当$2 \le p \le \sqrt{n}$且$p \nmid n$, 则n是素数.

素数

【例1.1.2】 n为37, 6≤$\sqrt{37}$, 小于6的素数有p=2, 3, 5, 用p去除37, p不整除37 , 故37为素数.

埃拉托色尼斯筛法

【例1.1.3】 找出所有小于等于50的素数.

解: 由性质②, 因为$7 < \sqrt{50} < 8$, 故依次划去2的倍数、3的倍数, 5的倍数和7的倍数, 剩下的数即为素数.

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~~

【人物传记】 埃拉托色尼斯

埃拉托色尼斯（公元前276-194）, 出生于希腊属地埃及西部的Cyrene, 他在雅典的柏拉图学习了一段时间. 托勒密二世（Ptolemy II）邀请他到亚历山大教他的儿子. 后来成为著名的亚历山大图书馆馆长. 他著有数学、地理、天文、历史、哲学和文学方面的书. 除了数学方面的工作, 他还以古代编年史和地理测量闻名.

素数的性质

③ 素数有无穷多.

证明: 用反证法. 假设只有有限个素数, 它们是$q_1, \ldots, q_k$.

考虑$m = q_1 \ldots q_k + 1$, 因为素数个数有限且为$q_1, \ldots, q_k$, 所以m必是合数, 从而知必存在素数q_i, 使得$q_i | m$. 由于$m = q_1 \ldots q_k + 1$, 故整除不可能的, 矛盾.

因此, 假设是错误的, 即素数必有无穷多个. 证毕.

素数个数定理

【定理1.1.1】 令$\pi(x)$表示不超过$x(x>0)$的素数的个数. 随着x的增大, $\pi(x)$和$x/\ln x$的比值趋于1. $\ln x$是x的自然对数. 即:

$$\lim_{x\to\infty}\pi(x)/(x/\ln x)=1$$

下面是对素数个数的统计。

x	$\pi(x)$	$x/\ln x$整数部分	$\pi(x)/(x/\ln x)$
1,000	168	145	1.16
100,000	9592	8686	1.10
10,000,000	664579	620241	1.07
1,000,000,000	50847478	48254942	1.05

【人物传记】 克里斯汀 · 歌德巴赫

克里斯汀·歌德巴赫（1690-1764）生于普鲁士哥尼斯堡（这个城市因七桥问题而在数学界很有名）. 1725年成为圣彼得堡皇家学院的数学教授. 1728年到莫斯科成为沙皇彼得二世的老师. 1742年任职于俄国外交部. 除了“每个大于2的偶数都能写为两个素数的和以及每个大于5的奇数能写为3个素数的和”的猜想外, 在数学分析方面也做出了令人瞩目的贡献.

【人物传记】 陈景润

陈景润（1933-1996）取得了关于孪生素数和歌德巴赫猜想的重要结果. 1966年发表《On the representation of a large even integer as the sum of a prime and the product of at most two primes》（《大偶数表为一个素数及一个不超过二个素数的乘积之和》,简称“1+2”）, 成为哥德巴赫猜想研究上的里程碑. 而他所发表的成果也被称之为陈氏定理.

【人物传记】 张益唐

美籍华裔数学家张益唐（1955-）于1978年进入北京大学数学科学学院攻读本科, 1982年读硕士, 师从潘承彪, 1985年入读普渡大学, 导师为莫宗坚. 2013年由于在研究孪生素数猜想上取得了重大突破, 于第六届世界华人数学家大会中荣获晨兴数学卓越成就奖, 后来他也获颁Ostrowski奖和Rolf Schock奖. 2014年, 美国数学学会更将崇高的柯尔数论奖授予张益唐. 同年7月4日, 张益唐当选为中央研究院第30届数理科学组院士. 同年9月, 张益唐获得了该年度的麦克阿瑟奖（俗称“天才”奖）.

1.2.1带余除法

【定理1.2.1】（带余除法）设a, b是两个给定的整数, $b > 0$. 那么, 一定存在唯一的一对整数q与r, 满足
$a = qb + r,\ 0 \le r < b.$

证明：（存在性）考虑一个整数序列

$\ldots, -3b, -2b, -b, 0, b, 2b, 3b, \ldots$

它们将实数轴分成长度为b的区间, 而a必定落在其中的一个区间中. 因此存在一个整数q使得$qb \le a < (q+1)b$.

令$r = a - qb$, 则有$a = qb + r,\ 0 \le r < b.$

(唯一性)如果分别有q, r和q_1, r_1满足

$a = qb + r,\ 0 \le r < b.$

$a = q_1 b + r_1,\ 0 \le r_1 < b.$

两式相减有$b(q - q_1) = -(r - r_1)$. 故$b | r - r_1$.

由已知, $0 \le r < b$, $0 \le r_1 < b$, 故$-b < r - r_1 < b$.

由$b | r - r_1$, $r = r_1$.

又因$q_1 b + r_1 = qb + r$, 故$q = q_1$.

在$a = qb + r, 0 \le r < b$中, 称q为a被b除所得的**不完全商**, 称r为a被b除所得的**余数**.

带余除法一般形式

【定义1.2.1】 设$a = qb + r,\ 0 \le r < b$, 称q为a被b除所得的不完全商, 称r为a被b除所得的余数.

【推论】 $b \mid a$的充要条件是a被b除所得的余数$r = 0$.

【定理1.2.2】 设a, b是两个给定的整数, $b \neq 0$, 则对任意整数c, 一定存在唯一的一对整数q与r, 满足

$$a = qb + r,\ c \le r < |b| + c.$$

这是欧几里德除法的一般形式.

带余除法-举例

【例1.2.1】 设$a=100$, $b=30$,

若$c=10$, 则$10\le r<40$, 即$100=3\times 30+10$;

若$c=35$, 则$35\le r<65$, 即$100=2\times 30+40$;

若$c=-50$, 则$-50\le r<-20$, 即$100=5\times 30+(-50)$.

1.2 .2 最大公因数

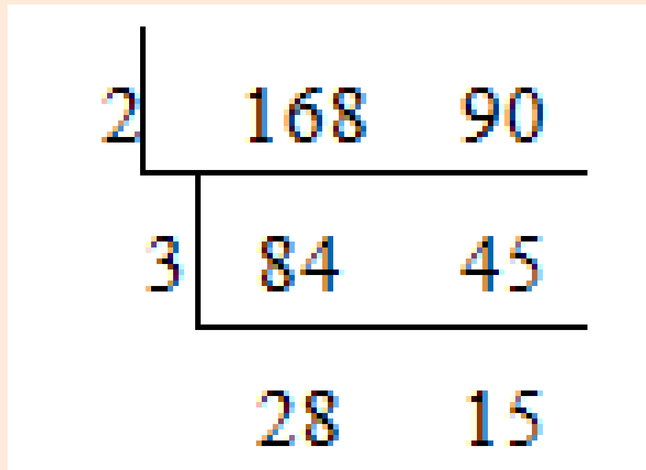
【定义1.2.2】 设a和b是两个整数. 若整数d是它们中每一个数的因数, 那么d就称做a和b的**公因数**（或公约数）.a和b的公因数中最大的一个叫做**最大公因数**, 记为(a, b). 也有的书记作gcd(a, b), 即greatest common divisor三个因为单词的首字母. 若(a, b)=1, 称a和b互素或互质.

进一步地, 若整数$a_1, a_2, \dots, a_n$不全为零, 那么$a_1, a_2, \dots, a_n$的公因数中最大的一个叫做最大公因数, 记作($a_1, a_2, \dots, a_n$). 当($a_1, a_2, \dots, a_n$)=1时, 称$a_1, a_2, \dots, a_n$互素. 注意, 这与$a_1, a_2, \dots, a_n$两两互素不同, $a_1, a_2, \dots, a_n$两两互素要求$(a_i, a_j) = 1, i \neq j$.

最大公因数-举例

【例1.2.2】 求最大公因数(168, 90).

解: 这里采用短除法求解. 我们知道, 一个整数要么是素数, 要么有不超过$\sqrt{n}$的素因数. 要求a和b的最大公因数, 可以依次用2, 3, 5, …去试除a和b. 若都能整除, 则找到公因数p_1, 然后用2, 3, 5, …去试除a/p_1和b/p_1…. 重复这个过程, 就可以找到a和b的所有公因数. 所有公因数的乘积即为a和b的最大公因数.



故168和99的最大公因数为(168, 90)=2×3=6.

最大公因数的基本性质

① $(a,b)=(b,a)$.

② 设a,b为正整数, 若$b\mid a$, 则$(a,b)=b$.

③ 设$a_1,a_2,\dots,a_n$是n个不全为零的整数, 则

（i） $a_1,a_2,\dots,a_n$与$|a_1|,|a_2|,\dots,|a_n|$的公因数相同;

（ii） $(a_1,a_2,\dots,a_n)=(|a_1|,|a_2|,\dots,|a_n|)$.

最大公因数的基本性质

④ 设a, b为正整数，则

$(a, b)＝(a, -b) = (-a, b) = (-a, -b)$.

⑤ $b \neq 0$, 则$(0, b)＝|b|$.

⑥ 设$m > 0$, $m(a_1, a_2, \ldots, a_n)= (ma_1, ma_2, \ldots, ma_n)$.

⑦ 设$a_1, a_2, \ldots, a_n$为整数，且$a_1 \neq 0$, 令$(a_1, a_2)= d_2$, $(d_2, a_3)= d_3$, …, $(d_{n-1}, a_n)= d_n$, 则$(a_1, a_2, \ldots, a_n)＝d_n$.

【例1.2.3】 计算最大公因数（120, 150, 210, 35）.

解: （120, 150）=30, （30, 210）=30, （30, 35）=5,

故（120, 150, 210, 35）=5

或（120, 150, 210, 35）=((120, 150), (210, 35))=(30,35) =5

最大公因数的基本性质

⑧ 设整数a, b, c，若$a|bc$且$(a, b) = 1$，则$a|c$.

⑨ 设整数a, b, c，若$c > 0$，则$(ac, bc) = (a, b)c$.

【例1.2.4】令$a = 5$, $b = 3$, $c = 10$. 5|3×10, (5,3)=1, 故5|10.

⑩ 设整数a, b, c，若$(a,\ c) = 1$, $(b,\ c) = 1$，则$(ab, c) = 1$.

⑪ 设整数a, b, 若$d > 0$, 若$d|a, d|b$, 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：因(a, b)= $(\frac{a}{d}, \frac{b}{d})d$, 故$\left(\frac{a}{d}, \frac{b}{d}\right) = \frac{(a,b)}{d}$.

特别地，当$d = (a, b)$, $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = \frac{(a,b)}{(a,b)} = 1$.

【例1.2.5】12和18的公因数是±1, ±2, ±3, ±6, 最大公因数(12,18)=6. 取$d = 2 > 0$, $\left(\frac{12}{2}, \frac{18}{2}\right) = (6,9) = 3$, $\frac{(12,18)}{2}$=$\frac{6}{2}$=3.

【人物传记】 欧几里德

【人物传记】 欧几里德（Euclid, 前325年—前265年）, 古希腊数学家, 他最著名的著作《几何原本》被广泛的认为是历史上最成功的教科书,从古至今已经有了上千种版本, 这本书介绍了从平面到刚体几何以及数论的知识. 人们关于欧几里德的生平所知很少, 现存的欧几里德画像都是出于画家的想像.

1.2.3 欧几里德算法

当两个数很大且共同的素因数也很大时, 短除法用起来就不方便了. 例如, 求46480和39423的最大公因数. 这里介绍另外一种求最大公因数的方法–**欧几里德算法**, 该方法有较高的效率, 而且易于程序实现.

欧几里德算法, 中文通常称为**辗转相除法**, 主要用于求两个整数的最大公因数, 从而为求解一次同余方程及一次同余方程组做铺垫.

欧几里德算法

【定理1.2.3】 设a, b, c是三个不全为零的整数，$a = bq + c$, 其中q是整数，则$(a, b) = (b, c)$.

证明: 设d $= (a, b), e = (b, c)$. 则因$d \mid a, d \mid b$, 知$d \mid a - bq = c$知d为c的因数，从而$d \leq e$.
同理可知$e \leq d$, 故$d = e$.

该定理给出了求最大公因数$d = (a, b)$的一个方法，下面介绍的欧几里德算法就是建立在此基础上的.

设整数$a > b > 0$, 记$r_0 = a, r_1 = b$, 反复利用带余除法:

$$r_0 = r_1 q_1 + r_2,\ 0 \le r_2 < r_1$$
$$r_1 = r_2 q_2 + r_3,\ 0 \le r_3 < r_2$$
……
$$r_{n-2} = r_{n-1} q_{n-1} + r_n,\ 0 \le r_n < r_{n-1}$$
$$r_{n-1} = r_n q_n + r_{n+1},\ r_{n+1} = 0$$

因为$a > r_1 > r_2 > \cdots > r_{n-1} > r_n > r_{n+1} \geq 0$, 故必存在$n$, 使得$r_{n+1} = 0$.

欧几里德算法

【定理1.2.4】 设整数$a > b > 0$, 则$(a, b) = r_n$, 其中r_n是带余除法中最后一个非零余数.

证明: 由【定理1.2.3】, $(a, b) = (r_0, r_1) = (r_1, r_2) = (r_2, r_3) = \cdots = (r_{n-1}, r_n) = (r_n, 0) = r_n$.

算法的题设要求$a > b > 0$, 若不满足题设, 由于$(a_1, a_2, \dots, a_n) = (|a_1|, |a_2|, \dots, |a_n|)$, 故可以通过计算$(|a|, |b|)$求得$(a, b)$.

欧几里德算法-举例

【例1.2.6】利用欧几里德算法求（172, 46）.

172=46×3+34	**(172, 46)=(46,34)**
46=34+12	(46,34)=(34,12)
34=12×2+10	(34,12)=(12,10)
12=10+2	(12,10)=(10,2)
10=5×2	(10,2)=(2,0)=2

欧几里德算法-举例

也可以这样求解：

172=46×4+(-12)	**(172, 46)=(46,-12)**
46=(-12)×(-4)+(-2)	(46,-12)=(-12,-2)
-12=6×(-2)	(-12,-2)=(-2,0)=2

C语言的一种程序实现方法

下面给出C语言的一种程序实现方法.

```
int gcd(int a, int b)
{
   while(b != 0)
   {  int r = b;  b = a % b;  a = r;   }
   return a;
}
```

【定义1.2.3】 设a与b是两个整数, 那么a与b的线性组合是形如$ma + nb$的和式, 其中m和n为整数.

裴蜀等式

【定理1.2.5】 设a, b为任意正整数, 则存在整数s, t, 使得 $(a, b) = sa + tb$.

对【定理1.2.5】的几点说明:

(1) 该定理的证明, 可直接由辗转相除法反推回去, 即得结论.

(2) 该等式也称为Bézout等式（**裴蜀等式**）.

(3) 整数s, t的取值有很多组, 每组s, t都称为**裴蜀数**.

(4) 上面这个表达式可以描述为: 整数a, b的线性和所能表示的最小的正整数是它们的最大公因数.

(5) 容易知道(a, b)的倍数也可以用a, b的线性和表示, 比如:

$m(a, b) = m(sa + tb) = (ma)s + (mb)t, m \in Z$.

下面证明: 整数a, b的线性和所能表示的最小的正整数是它们的最大公因数.

证明 设d是a与b线性组合所能表示的最小的正整数, 记为$d = ma + \mathrm{n}b$, m与n为整数. 证明过程分2步: (1) d是a与b的公因数; (2) d是a与b的最大公因数.

(1) 由带余除法, 存在整数q和r, 使$a = dq + r, 0 \leq r < d$. 故

$$r = a - dq = a - (ma + nb)q = (1 - qm)a - nqb$$

可见, r是a与b线性组合. 而d是a与b线性组合所能表示的最小的整数, 且$0 \leq r < d$, 故$r = 0$. 即$a = dq$. 故$d|a$.

类似可证$d|b$. 故d是a与b的公因数.

(2) 设c是a与b的任意一个公因数, 则$c|a$, $c|b$, 故$c|ma + nb = d$. 故$d \geq c$. 即d是a与b的最大公因数.

裴蜀等式-举例

【例1.2.7】有两个整数$a = 172$和$b = 46$, 求整数s, t, 使得$as + bt = (a, b)$时的s和t分别等于多少？

计算过程	备注
172=46×3+34	(172, 46)=(46,34)
46=34+12	(46,34)=(34,12)
34=12×2+10	(34,12)=(12,10)
12=10+2	(12,10)=(10,2)
10=5×2	(10,2)=(2,0)=2

裴蜀等式-举例

计算过程	备注
2=12-10	(12,10)=(10,2)
=12-（34-12×2）=12×3-34	(34,12)=(12,10)
=(46-34)×3-34=46×3-34×4	(46,34)=(34,12)
=46×3-(172-46×3)×4 =46×15-172×4	(172, 46)=(46,34)

故: 2=46×15+172×**(-4)**

容易知道, 在【例1.2.7】中, 2=46×(15+172×m)+172×(-4+46×(-m)), $m \in Z$, 仍然使等式成立. 故s, t的值不唯一. 下面这个定理给出了这种不定方程的所有解的表达式.

【定理1.2.6】 设a, b, c是整数且$d = (a, b)$, 对于方程$ax + by = c$, 如果d∤c ,那么方程没有整数解. 如果$d | c$, 则存在无穷多个整数解. 另外, 如果$x = x_0$,$y = y_0$是方程的一个特解, 那么所有的解可以表示为:$x = x_0 + (b/d)n$, $y = y_0 - (a/d)n$, n为整数.

裴蜀等式-特例

【定理1.2.6】 整数a, b互素当且仅当存在整数s, t, 使得$sa + tb = 1$.

证明: 必要性: 由【定理1.2.6】知成立.

充分性: 设$d = (a, b)$ 且有$sa + tb = 1$. 由$d \mid a, d \mid b$知$d \mid sa + tb = 1$, 故$d = 1$.

裴蜀等式-举例

【例1.2.8】 有两个整数$a = 40$和$b = 7$, 求整数s, t, 使得$as + bt = (a, b)$时的s和t分别等于多少？

解: 40=5×7+5, 7=5×1+2, 5=2×2+1

1=5-2×(7-5×1)=5×3-2×7

=(40-5×7)×3-2×7=40×3-17×7

=40×3+(-17)×7

在本例题中, 容易知道$(40, 7) = 1$, 但由$(\mathrm{a}, \mathrm{b}) = 1$是不容易看出线性表达式中的$s, t$的值.

```
void Euclid(unsigned int num1,unsigned int num2)
{
		int a[32],b[32];
		int inv_a,inv_b,tmp;
		int i=0,j=0;
		a[0]=num1;
		b[0]=num2;
	while(a[i]%b[j]!=0)
		{
			printf("%d=%d×%d+%d\n",a[i],a[i]/b[j],b[j],a[i]%b[j]);
			i++;
			j++;
			a[i]=b[j-1];
			b[j]=a[i-1]%b[j-1];
		}
	printf("%d=%d*%d+%d\n\n",a[i],a[i]/b[j],b[j],a[i]%b[j]);
```

```
////////////回代过程/////////////////////////////////////
        i--;j--;
        inv_a=1;
        inv_b=-a[i]/b[j];
        printf("%d\n",a[i]%b[j]);
        for(;i>=0,j>=0;i--,j--)
        {
                printf("  =%d×(%d)+%d×(%d)\n",a[i],inv_a,b[j],inv_b);
                tmp=inv_a;
                inv_a=inv_b;
                inv_b=tmp-a[i-1]/b[j-1]*inv_b;
        }
}
```

下面给出程序的一个运行结果：

$209=3\times59+32$

$59=1\times32+27$

$32=1\times27+5$

$27=5\times5+2$

$5=2\times2+1$

$2=2*1+0$

1

$=5\times(1)+2\times(-2)$

$=27\times(-2)+5\times(11)$

$=32\times(11)+27\times(-13)$

$=59\times(-13)+32\times(24)$

$=209\times(24)+59\times(-85)$

【定理1.2.7】 设a,b是任意两个正整数, 则

$s_n a + t_n b = (a,b)$.

对于$j = 2,\ldots,n$, 这里s_j, t_j归纳地定义为:

$$\begin{cases} s_0 = 1, s_1 = 0, s_j = s_{j-2} - q_{j-1}s_{j-1} \\ t_0 = 0, t_1 = 1, t_j = t_{j-2} - q_{j-1}t_{j-1} \end{cases}, j = 2,\ldots,n-1,n.$$

其中q_j是欧几里德算法中每一步的商, 即$r_{j-1} = r_j q_j + r_{j+1}$, $0 \le r_{j+1} < r_j$.

证明：只需证明：对于$j = 0, 1, 2, \dots, n-1, n$, $s_j a + t_j b = r_j$. 因为$(a, b) = r_n$, 所以$s_n a + t_n b = (a, b)$.

用数学归纳法证明.

当$j = 0$时, $s_0 = 1, t_0 = 0$, $s_0 a + t_0 b = a = r_0$, 结论成立;

当$j = 1$时, , $s_1 = 0, t_1 = 1$, $s_1 a + t_1 b = b = r_1$, 结论成立;

假设结论对于$1 \le j \le k-1$成立. 即

$s_j a + t_j b = r_j$.

对于$j = k$, 有 $r_k = r_{k-2} - r_{k-1} q_{k-1}$

利用归纳假设得到

$$r_k = (s_{k-2}a + t_{k-2}b) - (s_{k-1}a + t_{k-1}b)q_{k-1}$$

$=(s_{k-2} - q_{k-1}s_{k-1})a + (t_{k-2} - q_{k-1}t_{k-1})b$

$=s_k a + t_k b$.

因此, 结论对于$j = k$成立.

【定理1.2.8】 若$d > 0$是a与b的最大公因数, 则:

（1）$d|a, d|b$;

（2）若$e|a, e|b$, 则$e \mid d$.

证明 (1) 因d是a与b的最大公因数, 结论成立.

(2) 由【定理1.2.5】, 存在整数s, t, 使得$d = (a, b) = sa + tb$. 若$e|a, e|b$, 则$e \mid sa + tb = d$.

事实上, 从前面给出的短除法的求解过程, 可以直观理解结论.

作业1

1、设a为自己的学号，b=210，求整数s,t，使得 $as+tb=(a,b)$

1.3 最小公倍数

【定义1.3.1】 设$a_1, a_2, \dots, a_n$为整数, 若m是这些数的倍数, 则称m为这n个数的一个公倍数. 所有公倍数中最小的正整数叫做最小公倍数, 记作$[a_1, a_2, \dots, a_n]$.

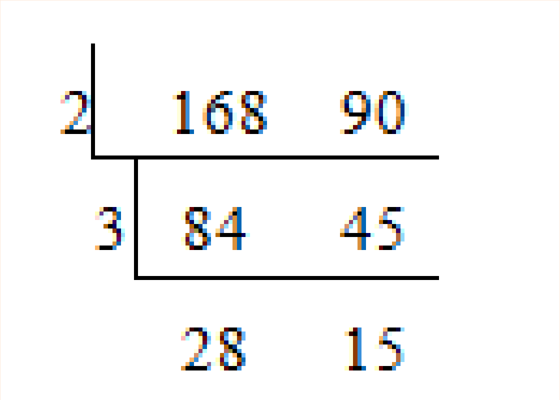
$m = [a_1, a_2, \dots, a_n]$ 可以等价定义为:

（i）$a_i | m, (1 \le i \le n)$;

（ii）若$a_i | m', (1 \le i \le n)$, 则$m | m'$.

【例1.3.1】 求最小公倍数[168, 90].

解: 前面用短除法得到了(168, 90). 求解过程如下.



故168和99的最小公倍数[168, 90]=2×3×28×15=2520.

最小公倍数的性质

① 设a,b是两个互素正整数，那么

（i）$a\mid m, b\mid m$，则 $ab\mid m$.

（ii）$[a,b]=ab$.

证明：（i）设若$a\mid m$，则$m=ak$. 又$b\mid m$，即$b\mid ak$. 而$(a,b)=1$，故$b\mid k$，即$k=bt, m=abt$，从而$ab\mid m$.

（ii）首先ab是a,b的公倍数. 其次由（i）和等价定义知ab是最小公倍数.

最小公倍数的性质

② 设a, b是两个正整数, 则$[a, b] = \frac{ab}{(a,b)}$.

证明: 令$\mathrm{d} = (a, b)$, 则$\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

由性质①, $\left[\frac{a}{d}, \frac{b}{d}\right] = \frac{a}{d} \cdot \frac{b}{d}$. 即$\left[\frac{a}{d}, \frac{b}{d}\right] d = \frac{a}{d} \cdot \frac{b}{d} \cdot d = \frac{ab}{d}$.

又知对任何整数$t > 0$, 有$t[a, b] = [ta, tb]$, 从而有

$[a, b] = \left[\frac{a}{d} \cdot d, \frac{b}{d} \cdot d\right] = \left[\frac{a}{d}, \frac{b}{d}\right] d = \frac{ab}{d}$.

这是求$[a, b]$的方法之一

最小公倍数的性质

③ 设a,b是两个正整数, 若$a\mid m, b\mid m$, 则 $[a,b]\mid m$.

证明: 令$\mathrm{d}=(a,b)$, 因$a\mid m,\ b\mid m$, 故$\frac{a}{d}\mid\frac{m}{d}, \frac{b}{d}\mid\frac{m}{d}$, 故$\frac{a}{d}\cdot\frac{b}{d}\mid\frac{m}{d}$, 于是$\frac{ab}{d}\mid m$.也即$[a,b]\mid m$.

【推论】 设$a_1,a_2,\dots,a_n$是n个整数, 如果$a_1|m$, $a_2|m, \dots, a_n|m$, 则$[a_1,a_2,\dots,a_n]|m$.

最小公倍数的性质

④ 设$a_1, a_2, \ldots, a_n$为整数, 令$[a_1, a_2] = m_2$, $[m_2, a_3] = m_3$, ..., $[m_{n-1}, a_n] = m_n$, 则 $[a_1, a_2, \ldots, a_n] = m_n$.

【例1.3.2】 求最小公倍数[120, 150, 210, 35].

解: $[120, 150] = \frac{120\times150}{(120,150)} = \frac{120\times150}{30} = 600$

$[600, 210] = \frac{600\times210}{(600,210)} = \frac{600\times210}{30} = 4200$

$[4200, 35] = \frac{4200\times35}{(4200,35)} = \frac{4200\times35}{35} = 4200$

故[120, 150, 210, 35]＝4200.

1.4算术基本定理

【定理1.4.1】（算术基本定理）任一整数$n > 1$都可以表示成素数的乘积. 且在不考虑乘积顺序的情况下, 该表达式是唯一的. 即

$$n = p_1 p_2 \cdots p_k, p_1 \le p_2 \le \cdots \le p_k.$$

【例1.4.1】 写出整数45, 49, 100, 128的因数分解式

解: 45＝3·3·5,　　49＝7·7,　　100＝2·2·5·5,

128＝2·2·2·2·2·2·2.

标准分解式

【定理1.4.2】 任一整数n>1都可以唯一地表示成

$n = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \ldots {p_k}^{\alpha_k}, \alpha_i > 0, i=1, 2, \ldots, k.$

其中$p_1 < p_2 < \cdots < p_k$且均为素数, 该等式叫做n的标准分解式.

【例1.4.2】 写出整数45, 49, 100, 128的标准分解式

解: 45＝$3^2 \cdot 5$， 49＝7^2， 100＝$2^2 \cdot 5^2$， 128＝2^7.

【定理1.4.3】 设整数n>1有标准分解式

$$n = {p_1}^{\alpha_1}{p_2}^{\alpha_2}\ldots{p_k}^{\alpha_k},\ \alpha_i > 0, i = 1, 2, \ldots, k.$$

若d是n的正因数, 则

$$d = {p_1}^{\beta_1}{p_2}^{\beta_2}\ldots{p_k}^{\beta_k},\ 0 \le \beta_i \le \alpha_i, i = 1, 2, \ldots, k.$$

最大公因数和最小公倍数

【定理1.4.4】 设正整数a,b的素因数分解式为

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\dots p_k^{\alpha_k},\ 0\le\alpha_i,\ i=1,2,\dots,k.$$

$$b=p_1^{\beta_1}p_2^{\beta_2}\dots p_k^{\beta_k},\ 0\le\beta_i,\ i=1,2,\dots,k.$$

令$r_i=\min(\alpha_i,\beta_i), s_i=\max(\alpha_i,\beta_i)$, 则有

$$(a,b)=p_1^{r_1}p_2^{r_2}\dots p_k^{r_k}.$$

$$[\mathrm{a},\mathrm{b}]=p_1^{s_1}p_2^{s_2}\dots p_k^{s_k}.$$

最大公因数和最小公倍数

【例1.4.3】 计算120, 150, 210, 35的最大公因数和最小公倍数.

解: $120 = 2^3 \cdot 3 \cdot 5$, $150 = 2 \cdot 3 \cdot 5^2$,

$210 = 2 \cdot 3 \cdot 5 \cdot 7$, $35 = 5 \cdot 7$.

$\therefore (120, 150, 210, 35) = 5$,

$[120, 150, 210, 35] = 2^3 \cdot 3 \cdot 5^2 \cdot 7 = 4200$.