信息平安数学根底

信息平安工程大学

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.

整除的一些根本性质

- 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 $a \pm b = mc \pm nc = (m \pm n)c$.

整除的一些根本性质

- 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, $6 \le \sqrt{37}$, 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

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

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

【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测的重要结果. 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”〕, 成为哥德巴赫猜测研究上的里程碑. 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. 2021年由于在研究孪生素数猜测上取得了重大突破, 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. 2021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, 张益唐中选为中央研究院第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〕.

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

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$qb \leq a < (q+1)b$.

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

带余除法一般形式

- 【定义1.2.1】 设$a = qb + r,\ 0 \leq r < b$, 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

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

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$100=3\times30+10$;

  若$c=35$, 则$35\le r<65$, 即$100=2\times30+40$;

  若$c=-50$, 则$-50\le r<-20$, 即$100=5\times30+(-50)$.

1.2 .2 最大公因数

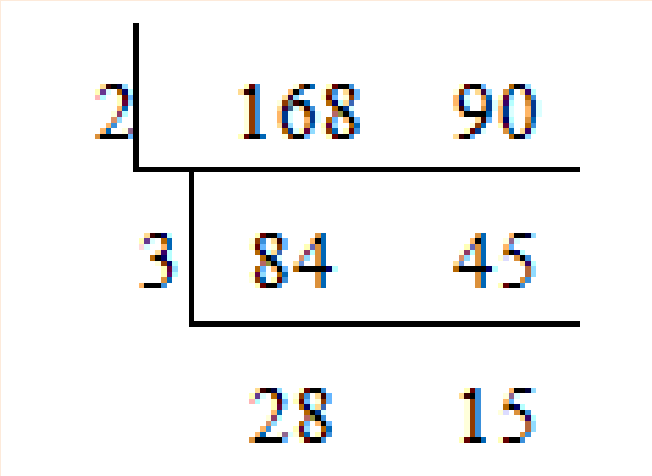
- 【定义1.2.2】 设a和b是两个整数. 若整数d是它们中每一个数的因数, 那么d就称做a和b的公因数（或公约数）.a和b的公因数中最大的一个叫做**最大公因数**, 记为(a, b). 也有的书记作gcd(a, b), 即greatest common divisor三个因为单词的首字母. 若(a, b)=1, 称a和b互素或互质.

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

最大公因数的根本性质

- ① $(a,b)=(b,a)$.

② 设a,b为正整数, 若$b \mid a$, 则$(a,b)=b$.

③ 设$a_1,a_2,\ldots,a_n$是n个不全为零的整数, 则

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

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

最大公因数的根本性质

- 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$(a_1, a_2) = d_2$, $(d_2, a_3) = d_3, \ldots, (d_{n-1}, a_n) = d_n$, 则$(a_1, a_2, \ldots, a_n) = d_n$.

【例】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

最大公因数的根本性质

- 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$(ab, c) = 1$.