

# 初等数论

整除, 同余和不定方程

珠海一中创美营 (数学)

2025 年 1 月 5 日

# 目录

# 目录

# 整除的概念与基本性质

对任给的两个整数  $a, b (a \neq 0)$ , 如果存在整数  $q$ , 使得  $b = aq$ , 那么称  $b$  能被  $a$  整除 (或称  $a$  能整除  $b$ ), 记作  $a \mid b$ . 否则, 称  $b$  不能被  $a$  整除, 记作  $a \nmid b$ .  
如果  $a \mid b$ , 那么称  $a$  为  $b$  的因数,  $b$  为  $a$  的倍数.

# 整除的概念与基本性质

## 性质 1.1

如果  $a \mid b$ , 那么  $a \mid (-b)$ , 反过来也成立; 进一步, 如果  $a \mid b$ , 那么  $(-a) \mid b$ , 反过来也成立.

# 整除的概念与基本性质

## 性质 1.1

如果  $a \mid b$ , 那么  $a \mid (-b)$ , 反过来也成立; 进一步, 如果  $a \mid b$ , 那么  $(-a) \mid b$ , 反过来也成立.

## 性质 1.2

如果  $a \mid b, b \mid c$ , 那么  $a \mid c$ . (传递性)

# 整除的概念与基本性质

## 性质 1.1

如果  $a \mid b$ , 那么  $a \mid (-b)$ , 反过来也成立; 进一步, 如果  $a \mid b$ , 那么  $(-a) \mid b$ , 反过来也成立.

## 性质 1.2

如果  $a \mid b, b \mid c$ , 那么  $a \mid c$ . (传递性)

## 性质 1.3

若  $a \mid b, a \mid c$ , 则对任意整数  $x, y$ , 都有  $a \mid bx + cy$ . (即  $a$  能整除  $b, c$  的任意一个“线性组合”)

## 例 1

若  $a|n$ ,  $b|n$ , 且存在整数  $x, y$ , 使得  $ax + by = 1$ , 证明:  $ab | n$ .



## 例 2

证明：无论在数 12008 的两个 0 之间添加多少个 3，所得的数都是 19 的倍数.

### 例 3

已知一个 1000 位正整数的任意连续 10 个数码形成的 10 位数是  $2^{10}$  的倍数. 证明: 该正整数为  $2^{1000}$  的倍数.

### 例 4

设  $m$  是一个大于 2 的正整数, 证明: 对任意正整数  $n$ , 都有  $2^m - 1 \nmid 2^n + 1$ .

# 素数与合数

## 性质 1.4

设  $n$  为大于 1 的正整数,  $p$  是  $n$  的大于 1 的因数中最小的正整数, 则  $p$  为素数.

# 素数与合数

## 性质 1.4

设  $n$  为大于 1 的正整数,  $p$  是  $n$  的大于 1 的因数中最小的正整数, 则  $p$  为素数.

## 性质 1.5

如果对任意 1 到  $\sqrt{n}$  之间的素数  $p$ , 都有  $p \nmid n$ , 那么  $n$  为素数. 这里  $n(> 1)$  为正整数.

# 素数与合数

## 性质 1.4

设  $n$  为大于 1 的正整数,  $p$  是  $n$  的大于 1 的因数中最小的正整数, 则  $p$  为素数.

## 性质 1.5

如果对任意 1 到  $\sqrt{n}$  之间的素数  $p$ , 都有  $p \nmid n$ , 那么  $n$  为素数. 这里  $n(> 1)$  为正整数.

## 证明.

事实上, 若  $n$  为合数, 则可写  $n = pq, 2 \leq p \leq q$ . 因此  $p^2 \leq n$ , 即  $p \leq \sqrt{n}$ . 这表明  $p$  的素因子  $\leq \sqrt{n}$ , 且它是  $n$  的因数, 与条件矛盾. 因此  $n$  为素数. □

# 素数与合数

## 性质 1.6

素数有无穷多个.

# 素数与合数

## 性质 1.6

素数有无穷多个.

## 证明.

若只有有限个素数, 设它们是  $p_1 < p_2 < \cdots < p_n$ . 考虑数

$$x = p_1 p_2 \cdots p_n + 1$$

其最小的大于 1 的因数  $p$ , 它是一个素数, 因此,  $p$  应为  $p_1, p_2, \cdots, p_n$  中的某个数. 设  $p = p_i, 1 \leq i \leq n$ , 并且  $x = p_i y$ , 则  $p_1 p_2 \cdots p_n + 1 = p_i y$ , 即

$$p_i(y - p_1 p_2 \cdots p_{i-1} p_{i+1} \cdots p_n) = 1.$$

这导致  $p_i \mid 1$ . 矛盾.

所以, 素数有无穷多个.





### 例 1

设  $n$  为大于 1 的正整数. 证明: 数  $n^5 + n^4 + 1$  不是素数.

## 例 2

考察下面的数列:

$$101, 10101, 1010101, \dots$$

问: 该数列中有多少个素数?

### 例 3

求所有的正整数  $n$ , 使得  $\frac{n(n+1)}{2} - 1$  是一个素数.

### 例 4

对任意正整数  $n$ ，证明：存在连续  $n$  个正整数，它们都是合数.

### 例 5

设  $n$  为大于 2 的正整数. 证明: 存在一个素数  $p$ , 满足  $n < p < n!$ .

## 例 6

设  $a, b, c, d, e, f$  都是正整数,  $S = a + b + c + d + e + f$  是  $abc + def$  和  $ab + bc + ca - de - ef - ed$  的因数. 证明:  $S$  为合数.

# 最大公因数与最小公倍数

## 带余数除法

设  $a, b$  是两个整数,  $a \neq 0$ , 则存在唯一的一对整数  $q$  和  $r$ , 满足

$$b = aq + r, 0 \leq r < |a|$$

其中  $q$  称为  $b$  除以  $a$  所得的商,  $r$  称为  $b$  除以  $a$  所得的余数.

### 性质 1.7 (贝祖 (Bezout) 定理)

设  $d = (a, b)$  , 则存在整数  $x, y$  , 使得

$$ax + by = d$$

### 性质 1.8

设  $d$  为  $a, b$  的公因数, 则  $d \mid (a, b)$  .

### 性质 1.9

设  $a, b$  是不全为零的整数, 则  $a$  与  $b$  互素的充要条件是存在整数  $x, y$  满足

$$ax + by = 1$$



### 性质 1.10

设  $a|c, b|c$  , 且  $(a, b) = 1$  , 则  $ab | c$  .

### 性质 1.11

设  $a | bc$  , 且  $(a, b) = 1$  , 则  $a | c$  .

### 性质 1.12

设  $p$  为素数,  $p | ab$  , 则  $p | a$  或  $p | b$  .

# 公倍数

设  $a, b$  都是不等于零的整数, 如果整数  $c$  满足  $a \mid c$  且  $b \mid c$ , 那么称  $c$  为  $a, b$  的公倍数. 在  $a, b$  的所有正的公倍数中, 最小的那个称为  $a, b$  的最小公倍数, 记作  $[a, b]$ .

### 性质 1.13

设  $a, b$  为非零整数,  $d, c$  分别是  $a, b$  的一个公因数与公倍数, 则  $d|(a, b), [a, b]|c$ .

### 性质 1.14

设  $a, b$  都是正整数, 则  $[a, b] = \frac{ab}{(a, b)}$ .

### 性质 1.15

$(a_1, a_2, a_3, \cdots, a_n) = ((a_1, a_2), a_3, \cdots, a_n)$  ;  
而  $[a_1, a_2, a_3, \cdots, a_n] = [[a_1, a_2], a_3, \cdots, a_n]$ .

### 性质 1.16

存在整数  $x_1, x_2, \dots, x_n$ , 使得

$$a_1 x_1 + a_2 x_2 + \dots + a_n x_n = (a_1, a_2, \dots, a_n)$$

### 性质 1.17

设  $m$  为正整数, 则

$$(ma_1, ma_2, \dots, ma_n) = m(a_1, a_2, \dots, a_n), \quad (1)$$

$$[ma_1, ma_2, \dots, ma_n] = m[a_1, a_2, \dots, a_n]. \quad (2)$$

## 例 1

设  $a, b$  为正整数, 且  $\frac{ab}{a+b}$  也是正整数. 证明:  $(a, b) > 1$ .

## 例 2

设正整数  $a, b, c$  满足  $b^2 = ac$ . 证明:  $(a, b)^2 = a(a, c)$ .

### 例 3

求所有的正整数  $a, b (a \leq b)$  , 使得

$$ab = 300 + 7[a, b] + 5(a, b). \quad (3)$$

### 例 4

求所有的正整数  $a, b$ , 使得

$$(a, b) + 9[a, b] + 9(a + b) = 7ab. \quad (4)$$



### 例 5

Fibonacci 数列定义如下:  $F_1 = F_2 = 1, F_{n+2} = F_{n+1} + F_n, n = 1, 2, \dots$ . 证明: 对任意正整数  $m, n$ , 都有  $(F_m, F_n) = F_{(m,n)}$ .

## 例 6

设  $n$  为大于 1 的正整数. 证明: 存在从小到大排列后成等差数列 (即从第二项起, 每一项与它前面那项的差为常数的数列) 的  $n$  个正整数, 它们中任意两项互素.

# 算术基本定理

## 定理 1 (算术基本定理)

设  $n$  是大于 1 的正整数, 则  $n$  可以分解成若干个素数的乘积的形式, 并且在不考虑这些素数相乘时的前后次序时, 这种分解是唯一的. 即对任意大于 1 的正整数  $n$ , 都存在唯一的一种素因数分解形式:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

这里  $p_1 < p_2 < \cdots < p_k$  为素数,  $\alpha_1, \alpha_2, \cdots, \alpha_k$  为正整数.

## 推论 2

设  $n$  的所有正因数 (包括 1 和  $n$ ) 的个数为  $d(n)$ , 那么

$$d(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdots (\alpha_k + 1)$$

## 推论 3

设  $n$  的所有正因数之和为  $\sigma(n)$ , 那么

$$\sigma(n) = (1 + p_1 + \cdots + p_1^{\alpha_1})(1 + p_2 + \cdots + p_2^{\alpha_2}) \cdots (1 + p_k + \cdots + p_k^{\alpha_k})$$

## 推论 4

设  $n, m$  的素因数分解分别为

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}, m = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k},$$

这里  $p_1 < p_2 < \cdots < p_k$ , 都为素数,  $\alpha_i, \beta_i$  都是非负整数, 并且对每个  $1 \leq i \leq k$ ,  $\alpha_i$  与  $\beta_i$  不全为零, 那么, 我们有  $(m, n) = p_1^{\gamma_1} p_2^{\gamma_2} \cdots p_k^{\gamma_k}$ ;  $[m, n] = p_1^{\delta_1} p_2^{\delta_2} \cdots p_k^{\delta_k}$ , 其中  $\gamma_i = \min \{\alpha_i, \beta_i\}$ ,  $\delta_i = \max \{\alpha_i, \beta_i\}$ ,  $1 \leq i \leq k$ .

### 例 17

在一个走廊上依次排列着编号为  $1, 2, \dots, 2012$  的灯共 2012 盏, 最初每盏灯的状态都是开着的. 一个好动的学生做了下面的 2012 次操作: 对  $1 \leq k \leq 2012$ , 该学生第  $k$  次操作时, 将所有编号是  $k$  的倍数的灯的开关都拉了一下. 问: 最后还有多少盏灯是开着的?(提示:  $44^2 = 1936, 45^2 = 2025$ )

### 例 18

求所有的正整数  $n$ , 使得  $n = d(n)^2$  .

### 例 19

设  $n$  为正整数. 证明: 数  $2^{2^n} + 2^{2^{n-1}} + 1$  至少有  $n$  个不同的素因子.



## 例 20

设  $m, n$  是正整数, 且  $m$  的所有正因数之积等于  $n$  的所有正因数之积. 问:  $m$  与  $n$  是否必须相等?

## 例 21

求所有的正整数  $x, y$ , 使得

$$y^x = x^{50}$$

## 例 22

给定正整数  $n > 1$ , 设  $d_1, d_2, \dots, d_n$  都是正整数, 满足:  $(d_1, d_2, \dots, d_n) = 1$ , 且对  $j = 1, 2, \dots, n$  都有  $d_j \mid \sum_{i=1}^n d_i$  (这里  $\sum_{i=1}^n d_i = d_1 + d_2 + \dots + d_n$ ).

(1) 证明:  $d_1 d_2 \cdots d_n \mid (\sum_{i=1}^n d_i)^{n-2}$ ;

(2) 举例说明:  $n > 2$  时, 上式右边的幂次不能减小.

# 目录

# 同余的概念与基本性质

同余是由大数学家高斯引入的一个概念. 我们可以将它理解为“余同”, 即余数相同. 正如奇数与偶数是依能否被 2 整除而得到的关于整数的分类一样, 考虑除以  $m(\geq 2)$  所得余数的不同, 可以将整数分为  $m$  类. 两个属于同一类中的数相对于“参照物”  $m$  而言, 具有“余数相同”这个性质. 这种为对比两个整数的性质, 引入一个参照物的思想是同余理论的一个基本出发点.

## 定义 1

如果  $a, b$  除以  $m(\geq 1)$  所得的余数相同, 那么称  $a, b$  对模  $m$  同余, 记作  $a \equiv b(\bmod m)$ . 否则, 称  $a, b$  对模  $m$  不同余, 记作  $a \not\equiv b(\bmod m)$ .

## 性质 2.1

$a \equiv b(\bmod m)$  的充要条件是  $m \mid a - b$ .

## 性质 2.2

若  $a \equiv b \pmod{m}$ ,  $c \equiv d \pmod{m}$ , 则  $a + c \equiv b + d \pmod{m}$ ,  
 $a - c \equiv b - d \pmod{m}$ ,  $ac \equiv bd \pmod{m}$ .

## 性质 2.2

若  $a \equiv b \pmod{m}$ ,  $c \equiv d \pmod{m}$ , 则  $a + c \equiv b + d \pmod{m}$ ,  
 $a - c \equiv b - d \pmod{m}$ ,  $ac \equiv bd \pmod{m}$ .

### 证明.

这些结论与等式的一些相关结论极其相似, 它们都容易证明. 我们只给出第 3 个式子的证明.

只需证明:  $m \mid ac - bd$ .

因为

$$ac - bd = ac - bc + bc - bd \quad (5)$$

$$= (a - b)c + b(c - d) \quad (6)$$

由条件  $m \mid a - b$ ,  $m \mid c - d$ , 知  $m \mid ac - bd$ . □



### 性质 2.3

若  $a \equiv b \pmod{m}$ ,  $n$  为正整数, 则  $a^n \equiv b^n \pmod{m}$  .

### 性质 2.4

若  $a \equiv b \pmod{m_1}$ ,  $a \equiv b \pmod{m_2}$  , 则  $a \equiv b \pmod{[m_1, m_2]}$  .

### 性质 2.5

若  $ab \equiv ac \pmod{m}$  , 则  $b \equiv c \pmod{\frac{m}{(a, m)}}$  .

## 性质 2.6

如果  $(a, m) = 1$  , 那么存在整数  $b$  , 使得  $ab \equiv 1(\text{mod } m)$  . 这个  $b$  称  $a$  对模  $m$  的数论倒数, 记为  $a^{-1}(\text{mod } m)$  , 在不会引起误解时常常简记为  $a^{-1}$  .

## 证明.

利用贝祖定理, 可知存在整数  $x, y$  使得

$$ax + my = 1$$

于是,  $m \mid ax - 1$  , 即  $ax \equiv 1(\text{mod } m)$  , 故存在符合条件的  $b$  .



## 例 2

求所有的素数  $p, q, r (p \leq q \leq r)$  , 使得

$$pq + r, pq + r^2, qr + p, qr + p^2, rp + q, rp + q^2$$

都是素数.

### 例 3

设  $n$  为大于 1 的正整数, 且  $1!, 2!, \dots, n!$  中任意两个数除以  $n$  所得的余数不同. 证明:  $n$  是一个素数.

### 例 4

设整数  $x, y, z$  满足

$$(x - y)(y - z)(z - x) = x + y + z. \quad (7)$$

证明:  $x + y + z$  是 27 的倍数.

### 例 5

是否存在 19 个不同的正整数, 使得在十进制表示下, 它们的数码和相同, 并且这 19 个数之和为 1999 ?

## 例 6

设  $m, n, k$  为正整数,  $n \geq m + 2$ ,  $k$  为大于 1 的奇数, 并且  $p = k \times 2^n + 1$  为素数,  $p \mid 2^{2^m} + 1$ . 证明:  $k^{2^{n-1}} \equiv 1 \pmod{p}$ .

# 剩余系及其应用

对任意正整数  $m$  而言, 一个整数除以  $m$  所得的余数只能是  $0, 1, 2, \dots, m-1$  中的某一个, 依此可将整数分为  $m$  个类 (例如  $m=2$  时, 就是奇数或偶数), 从每一类中各取一个数所组成的集合就称为模  $m$  的一个完全剩余系, 简称为模  $m$  的完系. 依此定义, 可以容易地得到下面的两个性质.



### 性质 2.7

若整数  $a_1, a_2, \dots, a_m$  对模  $m$  两两不同余, 则  $a_1, a_2, \dots, a_n$  构成模  $m$  的一个完系.

### 性质 2.8

任意连续  $m$  个整数构成模  $m$  的一个完系, 其中必有一个数为  $m$  的倍数.

引入完系的概念, 蕴含了“整体处理”的思想, 在用同余方法处理数论问题时, 我们常常需要选择不同的完系来达到目的, 做出恰当地分析.

## 例 1

证明: 在十进制表示下, 任意 39 个连续正整数中, 必有一个数的数码和是 11 的倍数.

## 例 2

设  $n$  为正奇数. 证明: 数

$$2 - 1, 2^2 - 1, \dots, 2^{n-1} - 1$$

中必有一个数是  $n$  的倍数.

### 例 3

设  $m, n$  为正整数,  $m$  为奇数, 且  $(m, 2^n - 1) = 1$ . 证明: 数  $1^n + 2^n + \cdots + m^n$  是  $m$  的倍数.

#### 例 4

(1) 证明: 存在无穷多组整数  $(x, a, b, c)$ , 使得

$$x^2 + a^2 = (x+1)^2 + b^2 = (x+2)^2 + c^2$$

(2) 问: 是否存在整数组  $(x, a, b, c, d)$ , 使得

$$x^2 + a^2 = (x+1)^2 + b^2 = (x+2)^2 + c^2 = (x+3)^2 + d^2?$$

### 例 5

设  $n$  为正整数. 证明: 存在一个各数码都是奇数的正整数, 它是  $5^n$  的倍数.

## 定理 1 (Fermat 小定理)

设  $p$  为素数,  $a$  为整数, 则  $a^p \equiv a \pmod{p}$ . 特别地, 若  $p \nmid a$ , 则  $a^{p-1} \equiv 1 \pmod{p}$ .

## 定理 1 (Fermat 小定理)

设  $p$  为素数,  $a$  为整数, 则  $a^p \equiv a \pmod{p}$ . 特别地, 若  $p \nmid a$ , 则  $a^{p-1} \equiv 1 \pmod{p}$ .

### 证明.

当  $p \mid a$  时, 结论显然成立.

当  $p \nmid a$  时, 设  $x_1, x_2, \dots, x_{p-1}$  是  $1, 2, \dots, p-1$  的一个排列, 我们先证:  $ax_1, ax_2, \dots, ax_{p-1}$  中任意两个数对模  $p$  不同余.

事实上, 若存在  $1 \leq i < j \leq p-1$ , 使得  $ax_i \equiv ax_j \pmod{p}$ , 则  $p \mid a(x_i - x_j)$ , 而  $p \nmid a$ , 故  $p \mid x_i - x_j$  (注意, 这里用到  $p$  为素数), 但  $x_i$  与  $x_j$  对模  $p$  不同余, 矛盾.

又  $ax_1, ax_2, \dots, ax_{p-1}$  中显然没有一个数为  $p$  的倍数, 因此,  $ax_1, ax_2, \dots, ax_{p-1}$  除以  $p$  所得的余数是  $1, 2, \dots, p-1$  的一个排列, 利用同余的性质, 知

$$(ax_1)(ax_2) \cdots (ax_{p-1}) \equiv x_1 x_2 \cdots x_{p-1} \pmod{p}$$

再由  $x_1 x_2 \cdots x_{p-1} = (p-1)!$ , 它不是  $p$  的倍数 (注意, 这里再次用到  $p$  为素数), 所以,  $a^{p-1} \equiv 1 \pmod{p}$ .





## 例 2

设  $n$  为正整数. 证明:  $7 \mid 3^n + n^3$  的充要条件是  $7 \mid 3^n n^3 + 1$ .

### 例 3

设  $x$  为整数,  $p$  是  $x^2 + 1$  的奇素因数, 证明:  $p \equiv 1 \pmod{4}$  .

### 例 4

设  $x$  为整数,  $p$  是数  $x^6 + x^5 + \cdots + 1$  的素因数. 证明:  $p = 7$  或  $p \equiv 1 \pmod{7}$ .

### 例 5

设  $p$  为素数. 证明: 存在无穷多个正整数  $n$ , 使得  $p \mid 2^n - n$ .

## 例 6

由 Fermat 小定理知, 对任意奇素数  $p$ , 都有  $2^{p-1} \equiv 1 \pmod{p}$ . 问: 是否存在合数  $n$ , 使得  $2^{n-1} \equiv 1 \pmod{n}$  成立?

### 例 7

求所有的素数  $p$ , 使得  $\frac{2^{p-1}-1}{p}$  是一个完全平方数.

### 性质 2.9

完全平方数  $\equiv 0$  或  $1 \pmod{4}$  , 奇数的平方  $\equiv 1 \pmod{8}$  .

### 性质 2.10

相邻两个完全平方数之间没有一个正整数是完全平方数. (这个性质经常用来证明某一类数不是完全平方数)

### 性质 2.11

若两个互素的正整数之积是完全平方数, 则这两个数都是完全平方数.

### 例 1

设素数从小到大依次排列为  $p_1, p_2, \dots$ . 证明: 对任意大于 1 的正整数  $n$ , 数  $p_1 p_2 \cdots p_n - 1$  和  $p_1 p_2 \cdots p_n + 1$  都不是完全平方数.



## 例 2

已知正整数  $a, b$  满足关系式

$$2a^2 + a = 3b^2 + b$$

证明:  $a - b$  和  $2a + 2b + 1$  都是完全平方数.

### 例 3

设正整数  $x, y, z$  满足  $(x, y, z) = 1$  , 并且  $\frac{1}{x} + \frac{1}{y} = \frac{1}{z}$ . 证明:  $x + y, x - z, y - z$  都是完全平方数.

### 例 4

求所有的素数  $p$ ，使得  $p^3 - 4p + 9$  是一个完全平方数.

### 例 5

已知  $n$  为正整数, 且  $2n+1$  与  $3n+1$  都是完全平方数. 证明:  $40 \mid n$ .

## 例 6

若  $a, b$  是使得  $ab + 1$  为完全平方数的正整数, 则记  $a \sim b$ . 证明: 若  $a \sim b$ , 则存在正整数  $c$ , 使得  $a \sim c, b \sim c$ .

### 例 7

求所有的正整数数对  $(a, b)$ , 使得

$$a^3 + 6ab + 1, b^3 + 6ab + 1$$

都是完全立方数.

### 例 8

求最小的正整数  $n$ , 使得存在整数  $x_1, x_2, \dots, x_n$ , 满足

$$x_1^4 + x_2^4 + \dots + x_n^4 = 1599$$

# 目录