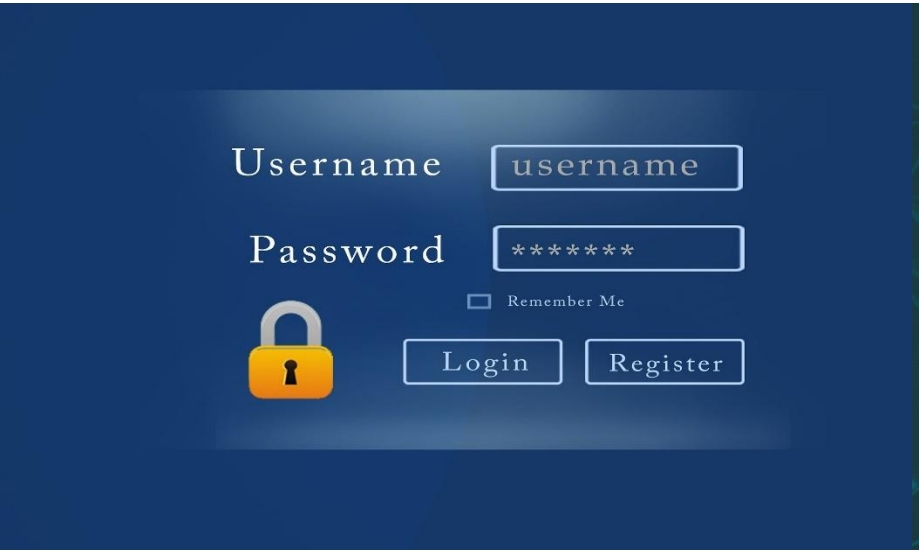
第1章 数论及应用

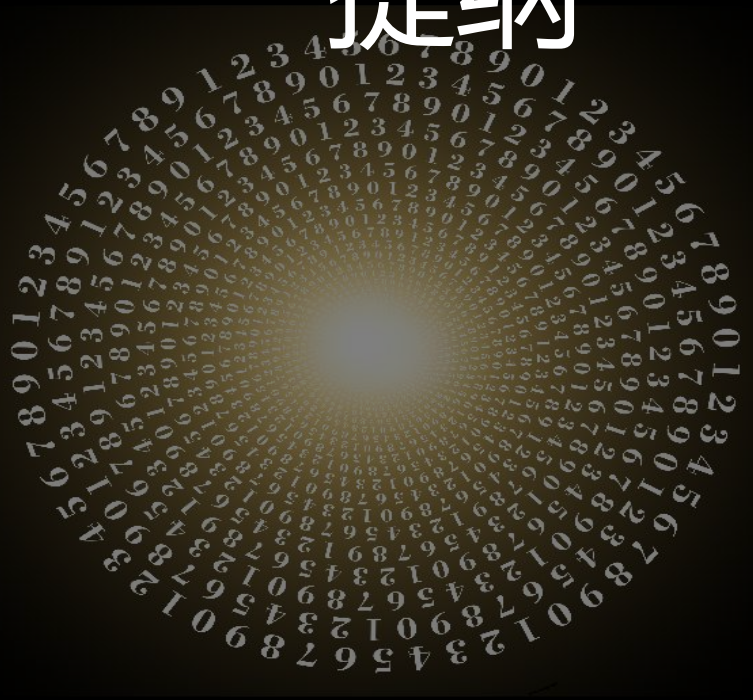
——从古老智慧到现代密码学

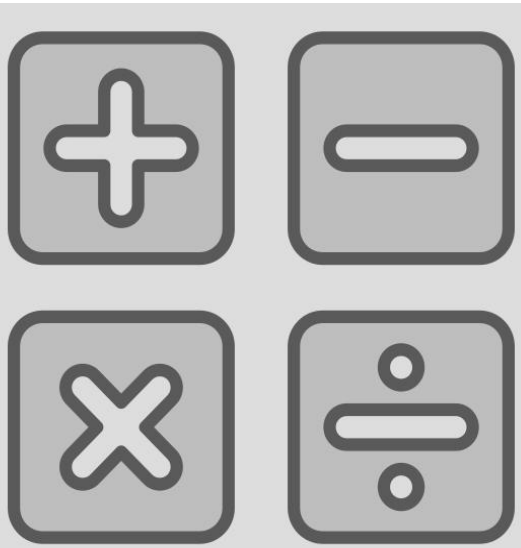
崔金华
邮箱:jhcui@hust.edu.cn
主页: https://csjhcui.github.io/
办公地址:华中科技大学南一楼东406室



致谢:课件主要参考《 Discrete Mathematics and its application》(Seventh Edition) Keneth H. Rosen 和《离散数学》(第2版) 屈婉玲,耿素云,张立昂版本的相关课件, 特此致谢!

Contents
提纲





第1.1节 整除性和模计算

Section 1.1: Divisibility and Modular Arithmetic

第1.1节 整除性和模计算

❑知识要点概览

1. 整除

整除的定义与性质，因子与倍数的概念

2. 除法算法

带余除法及其在实际问题中的应用

3. 模运算

同余关系的定义、性质及应用

4. 模m算术

模加法、模乘法及其代数性质

这些概念不仅是数学理论的基石，也在**密码学、哈希函数**和**随机数生成**等领域有广泛应用。

1.1.1 整除

- 【定义】: 如果a和b是整数, 且$a \neq 0$. 我们称为a**整除**b (或者b被a整除), 如果有整数c使得$b = ac$, 或者等价地$\frac{b}{a}$是一个整数.
- 当a整除b时, 我们称a是b的一个**因子**或除数, 而b是a的一个**倍数**. 用记号$a|b$表示a整除b. 当a不能整除b时, 则写作$a \nmid b$.
- 任何大于1的正整数都有两个**正因子**: 1和它自身, 称为它的**平凡因子**. 除平凡因子以外的其他因子称作**真因子**.

1.1.1 整除

- 例: 判断以下是否成立.

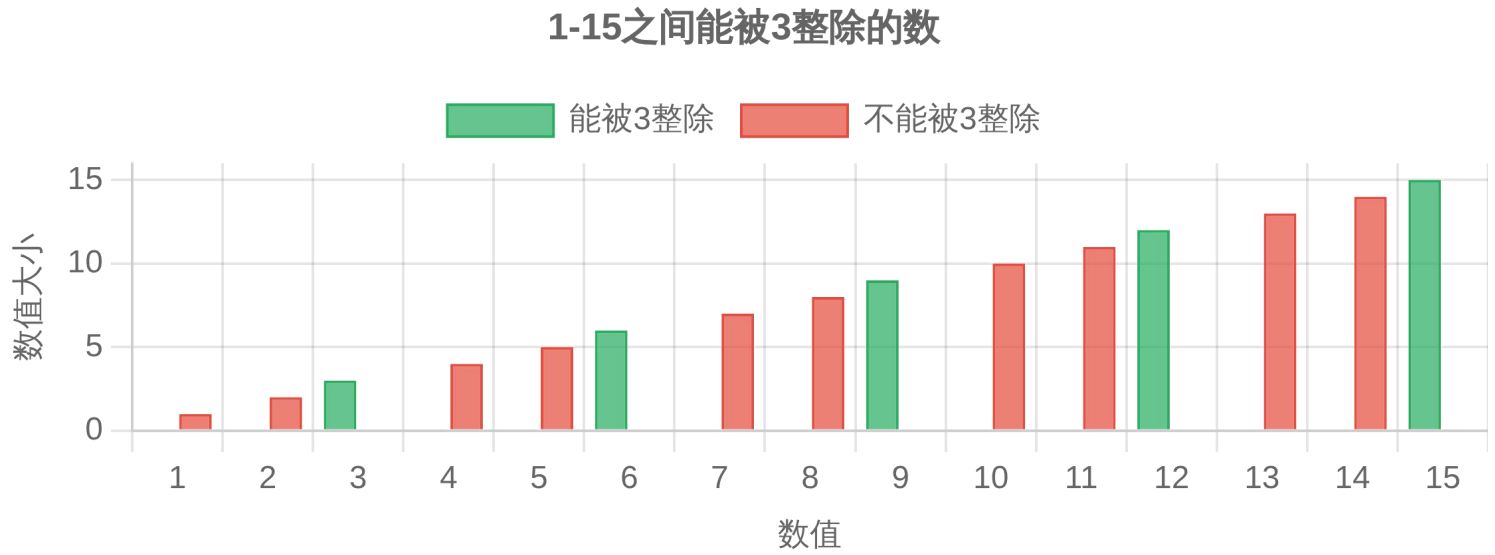
关系	判断	理由
3|12		
3|7		
5|0		

- 解:

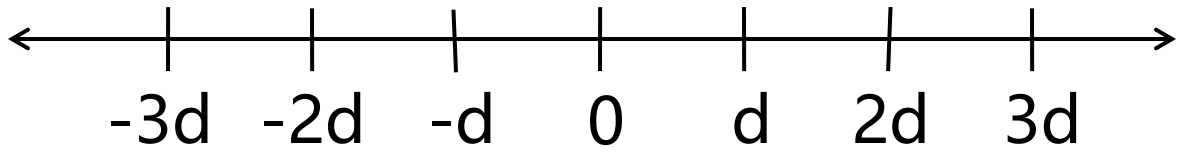
关系	判断	理由
3|12	成立	$12 = 3 \times 4$
3|7	不成立	$7 = 3 \times 2 + 1$
5|0	成立	$0 = 5 \times 0$

1.1.1 整除

- 整除关系可视化



- 当我们使用数轴来显示哪些整数能被正整数d整除



1.1.1 整除性质

- 【定理1】: 令 $a,\ b,\ c$ 为整数, 其中$a \neq 0$.
  - (i)如果$a|b$, $a|c$, 则 $a|(b\ +\ c)$;
  - (ii)如果$a|b$, 那么对所有的整数c都有$a|bc$;
  - (iii)如果$a|b$, $b|c$, 则$a|c$.
- 例:证明上述定理.
- 解:
  - (i)假定$a \mid b$, $a \mid c$, 则从整除的定义可知, 存在整数s和t, 满足$b = as$ 和 $c\ =\ at$. 因此, $b\ +\ c\ =\ as\ +\ at\ =\ a(s\ +\ t)$. 于是$a \mid (b\ +\ c)$.
  - (ii)假定$a \mid b$, 那么存在整数m, 满足$b = am$. 那么对于整数c, 满足$bc = amc$. 于是$a|bc$.
  - (iii)假定$a \mid b$, $b \mid c$, 那么存在整数m和n, 满足$b = am$, $c = bn$. 于是$c = amn$, 则 $a \mid c$.

1.1.1 整除性质

- 【推论】: 如果 a, b, c 是整数, 其中$a \neq 0$, 使得 $a \mid b$ 和$a \mid c$, 那么当m和n是整数时, 有$a|mb + nc.$
- 例:证明以上推论正确.
- 解:采用直接证明法. 由定理中(ii)可知, 当m和n是整数时有$a|mb$和$a|nc.$再由定理中(i)可得$a|mb + nc.$

1.1.2 除法算法

- **除法算法**: 令a为整数, d为正整数, 则存在唯一的整数q和r, 满足$0 \leq r < d$, 使得$a = dq + r$(该式子也称作**带余除法**). 其中a称为**被除数**, d称为**除数**, q称为**商**, r称为**余数**. 下面用记号表示商和余数:

$$q = a \textbf{ div } d$$

$$r = a \textbf{ mod } d$$

- 如果$d|a$，当且仅当(充要条件, 逻辑与证明章节会再细讲) a **mod** d =0.

重要性

除法算法是数论中的基础定理，为模运算、最大公约数等概念提供理论基础. 它保证了在整数除法中，总能得到唯一的商和余数.

1.1.2 除法算法

- 例:当101除以11时的商和余数是多少?
- 解:我们知道101=11*9+2. 因此, 101除以11的商为9= 101 **div** 11, 而余数为2 = 101 **mod** 11.

- 例:当-11除以3时的商和余数是多少?
- 解:我们知道-11=3*(-4)+1. 因此, -11除以3的商为−4 = −11 **div** 3, 而余数为1 = −11 **mod** 3.
- 【易错题. 注意余数要大于等于0, 所以这儿不是-11=3*(-3)-2】

1.1.2 除法算法

- 例:现在是星期二，那么100天后是星期几？【时间计算问题】
- 解:设星期日、一、二、…、六分别用0、1、2、…、6表示. 星期二用数字2表示. 100天后相当于经过了100 ÷ 7 = 14余2天, 即14个完整的星期加上2天. 所以100天后是, (2 + 2) mod 7 = 4，即星期四.

1.1.3 模运算

- 有时我们只对余数感兴趣. 为此, 引入新的特殊的记号来表示两个整数除以正整数m具有同样的余数.
- 【定义】: 如果a和b为整数, 而m为正整数, 则当m整除$a-b$时, 称**a模m同余b**, 或者称**a和b是模m同余的**, 记作$a \equiv b \ (mod\ m)$. 我们称$a \equiv b \ (mod\ m)$为**同余式**, 而m是它的**模**. 如果a和b不是模m同余的,则记作$a \not\equiv b \ (mod\ m)$.
- 例如a =17, b =5, m =6. 存在6|(17-5), 所以17 ≡ 5 $(mod\ 6)$
- 理解:同余的概念是用来表示两个整数(a和b)除以正整数m时具有同样的余数; a除以m的余数=b除以m的余数; $a-b$除以m等于一个整数; m整除$a-b$

1.1.3 模运算

- 同余关系是一种等价关系，具有以下性质：
- **反身性**(或称自反性): $a \equiv a \ (mod\ m)$
- **对称性**: 若$a \equiv b \ (mod\ m)$，则$b \equiv a \ (mod\ m)$
- **传递性**: 若$a \equiv b \ (mod\ m)$ 且$b \equiv \mathrm{c} \ (mod\ m)$，则$a \equiv \mathrm{c} \ (mod\ m)$

【基础知识：等价关系定义. 设R是非空集合A上的二元关系, 若R是自反的、对称的、传递的，则称R是A上的等价关系】

1.1.3 模运算

- 例:判断17是否模6同余5, 24是否模6同余14.
- 解:
  - 由于6整除17-5=12, 所以$17 \equiv 5 (mod\ 6)$;
  - 因为24-14=10不能被6整除, 所以$24 \not\equiv 14 (mod\ 6)$.

- 模运算的应用:
  - 时钟计时系统（模12或模24）
  - 周期性事件的计算
  - 哈希函数：将数据映射到固定长度的值
  - 密码学：RSA加密算法基于模运算
  - ……

1.1.3 模运算

- mod符号区别: 尽管$a \equiv b (mod\ m)$和a **mod** $m = b$中都包含“mod”，但是它们表示的是本质上不同的概念.
  - $a \equiv b\ (mod\ m)$ 表示两个整数间的关系;
  - a **mod** $m = b$ 表示一个函数.
- 可见关系式$a \equiv b (mod\ m)$和函数a **mod** m又紧密相关, 正如如下定理描述.

- 【定理3】: 令a和b为整数, 并令m为正整数, 则 $a \equiv b\ (mod\ m)$当且仅当a **mod** $m = b$ **mod** m.
- 例: 17 ≡ 5 $(mod\ 6)$, 因为17 **mod** 6=5 **mod** 6=5

1.1.3 模运算

- 【定理4】：令m为正整数，整数a和b是模m同余的当且仅当存在整数k使得$a = b + km$.
- 所有和a模m同余的整数集合称为a模m的**同余类**
- 例:证明上述定理.
- 解:
  - 如果$a \equiv b \pmod{m}$，由同余的定义可知$m \mid a-b$．这表示存在整数k使得$a-b = km$，于是$a = b + km$.
  - 反之，如果存在整数k使得$a = b + km$，则$km = a-b$. 综上所述，m整除$a-b$，所以$a \equiv b \pmod{m}$.

1.1.3 模运算

- 【总结】要说明整数a和b是模m同余，可以通过以下三种方式：
  - 1、$m|(a-b)$，m整除$a-b$
  - 2、$a \bmod m = b \bmod m$，两个整数进行求**mod**函数得到的余数是相同的
  - 3、存在整数k使得，$a = b + km$.

1.1.3 模运算

- 同余满足加法和乘法.
- 【定理5】: 令m为正整数. 如果 $a \equiv b \,(mod\, m), c \equiv d \,(mod\, m)$, 那么则有$a + c \equiv b + d \,(mod\, m)$ 且 $ac \equiv bd \,(mod\, m)$
- 这意味着模运算对加法和乘法是封闭的. 例如$7 \equiv 2 \,(mod\ 5)$, $11 \equiv 1 \,(mod\ 5)$, 那么有$18 \equiv 3 \,(mod\ 5)$且$77 \equiv 2 \,(mod\ 5)$
- 例:证明上述定理.
- 解(直接证明法): 因为$a \equiv b \,(mod\, m), c \equiv d \,(mod\, m)$, 由定理4可知存在整数$s$和$t$, 使得 $b = a + sm$ 和 $d = c + tm.$

1.1.3 模运算

- 解(续):

于是，$b + d = (a + sm) + (c + tm) = (a + c) + m(s + t)$ 且 $bd = (a + sm)(c + tm) = ac + m(at + cs + stm)$. 因此 $a + c \equiv b + d \pmod{m}$ 且 $ac \equiv bd \pmod{m}$.

1.1.3 模运算

- 在处理同余时必须小心, 有时我们可能想当然地认为为真的性质其实为假.
  - 如果$a * c \equiv b * c \ (mod\ m)$, 同余式$a \equiv b \ (mod\ m)$ 可能为假.
  - 如果$a \equiv b \ (mod\ m)$, $c \equiv d \ (mod\ m)$, 同余式$a^c \equiv b^d (mod\ m)$ 可能为假.
  - 思考: 如果$a \equiv b \ (mod\ m)$, 对于任意正整数c, 同余式$a^c \equiv b^c (mod\ m)$ 是否成立?【模运算的幂运算性质】
- 例: 存在同余式14 ≡ 8 $(mod\ 6)$. 因为6能整除14-8. 但是两边除以2得到新的同余式7 ≡ 4 $(mod\ 6)$却不成立. 这是因为6不能够整除7-4.

1.1.3 模运算

- 利用每个整数的**mod** m函数找出两个整数的和与积的该函数值:
- 【推论2】：令m为正整数，令a和b为整数，则 $(a + b)$ **(mod** m**)** = **((**a **mod** m**) + (**b **mod** m**)) mod** m，并且ab **mod** m = **((**a **mod** m**) (**b **mod** m**)) mod** m.

- 证明: 根据定义，可得$a \equiv (a \bmod m)(mod\ m)$ (因为a除以m的余数和 a **mod** m 除以m的余数是相同的，其中a **mod** m表示a除以m的余数)和 $b \equiv (b \bmod m)(mod\ m)$

  因此，根据定理5可得$(a + b) \equiv (a \bmod m) + (b \bmod m)(mod\ m)$和 $ab \equiv (a \bmod m)(b \bmod m)(mod\ m)$

1.1.4 模m算术

- 在Z_m(Z_m 为小于m的非负整数{0,1, …., $m-1$})上定义模m算术运算:
- 【**模m加法定义**】: 定义Z_m整数的加法(用$+_m$表示)为$a +_m b = (a + b)$ **mod** m, 这里等式右边的加法是普通的整数加法.
- 【**模m乘法定义**】: 整数的乘法(用表示$\cdot_m$)为$a \cdot_m b = (a * b)$ **mod** m, 这里等式的右边的乘法是普通的整数的乘法.

1.1.4 模m算术

- 生活中的模m运算, 时钟系统.

时钟是模12运算的完美例子:
10点后3小时是1点：$10 +_{12} 3 = 1$ (**mod** 12)
每隔12小时，时针回到相同位置

1.1.4 模m算术

- 例: 利用模m加法和乘法的定义, 计算$7 +_{11} 9$和 $7 \cdot_{11} 9$.
- 解:
  - 利用模11的加法和乘法定义, 我们可得
  - $7 +_{11} 9 = (7 + 9) \ \mathbf{mod}\ 11 = 16 \ \mathbf{mod}\ 11 = 5.$
  - $7 \cdot_{11} 9 = (7 \times 9) \ \mathbf{mod}\ 11 = 63 \ \mathbf{mod}\ 11 = 8.$

1.1.4 模m算术

- 模m算术满足以下性质.
  - **封闭性**: 如果a和b属于Z_m，则 $a +_m b$ 和 $a \cdot_m b$ 也属于 Z_m.
  - **结合律**: 如果 a, b, c 属于Z_m，则$(a +_m b) +_m c = a +_m (b +_m c)$ 和 $(a \cdot_m b) \cdot_m c = a \cdot_m (b \cdot_m c)$.
  - **交换律**: 如果a和b属于Z_m,那么$a +_m b = b +_m a$ 和 $a \cdot_m b = b \cdot_m a$.
  - **分配律**: 如果a, b, c 属于Z_m，则$a \cdot_m (b +_m c) = (a \cdot_m b) +_m (a \cdot_m c)$ 和 $(a +_m b) \cdot_m c = (a \cdot_m c) +_m (b \cdot_m c)$.
  - **单位元**: 元素0和1分别是模m加法和乘法的单位元. 即如果a属于Z_m, 则$a +_m 0 = a$ 和 $a \cdot_m 1 = a$.
  - **加法逆元**: 如果$a \neq 0$属于Z_m, 则$m - a$是a的模m加法逆元, 而0是其自身的加法逆元, 即$a +_m (m - a) = 0$ 且 $0 +_m 0 = 0$.
- 以上性质的证明留作自学练习. 注意有加法逆元, 但没有包括类似的乘法逆元, 因为模m乘法逆元并不一定存在. 例如2的模6乘法逆元不存在.

【基础知识:对于任意数a, 存在加法逆元(或称相反数, 或称反数)满足其与a的和为0】