蘇州大學
SOOCHOW UNIVERSITY

Chap4 Number Theory

Part I: Modular, Representation, and Prime

Jin-Hui Wu

2026-03-26

大纲

- 整除和模
- 整数表示和算法
- 素数和最大公约数
- 同余方程
- 同余的应用
- 密码学

大纲

- 整除和模 (4.1)
- 整数表示和算法
- 素数和最大公约数
- 同余方程
- 同余的应用
- 密码学

整除

- 整除
  - a整除b (a divides b)
    - a, b为整数，$a \neq 0$，且存在整数c，使得$b = ac$
    - 记作$a \mid b$，否则记作$a \nmid b$

整除

- 整除
  - a整除b (a divides b)
    - a, b为整数，$a \neq 0$，且存在整数c，使得$b = ac$
    - 记作$a \mid b$，否则记作$a \nmid b$
    - a是b的因子 (factor) 或除数 (divisor)
    - b是a的倍数 (multiple)

例

- 判断下列各式是否成立
  - $3 \mid 7$
  - $4 \mid 12$

- a, b为整数，$a \neq 0$，且存在整数c，使得$b = ac$
- 记作$a \mid b$，否则记作$a \nmid b$

整除

- 整除
  - a整除b (a divides b)
    - a, b为整数，$a \neq 0$，且存在整数c，使得$b = ac$
    - 记作$a \mid b$，否则记作$a \nmid b$
  - 整除的性质
    - $a|b \wedge a|c \Rightarrow a|(b+c)$
    - $a|b \Rightarrow \forall c \in \mathbb{Z}\,(a|bc)$
    - $a|b \wedge b|c \Rightarrow a|c$

模算术

- 同余 (congruence)
  - $a, b \in \mathbb{Z}$，$m \in \mathbb{Z}^+$，若$m|(a-b)$，则称a模m同余b (a is congruent to b modulo m)
  - 记作$a \equiv b \pmod{m}$
  - 同余：a和b除以m的余数相同

例

- 判断下列各式是否成立
  - $17 \equiv 5 \pmod 6$
  - $24 \equiv 14 \pmod 6$

- $a, b \in \mathbb{Z}$，$m \in \mathbb{Z}^+$，若$m|(a-b)$，则称a模m同余b (a is congruent to b modulo m)
- 记作$a \equiv b \pmod m$

模算术

- 同余 (congruence)
  - $a, b \in \mathbb{Z}$，$m \in \mathbb{Z}^+$，若$m|(a-b)$，则称a模m同余b (a is congruent to b modulo m)
  - 记作$a \equiv b \pmod{m}$
  - 同余的性质
    - m为整数，则$a \equiv b \pmod{m} \Leftrightarrow \exists k \in \mathbb{Z}\ \text{s.t.}\ a = b + km$

模算术

- 同余 (congruence)
  - $a, b \in \mathbb{Z}$，$m \in \mathbb{Z}^+$，若$m|(a-b)$，则称a模m同余b (a is congruent to b modulo m)
  - 记作$a \equiv b \pmod{m}$
  - 同余的性质
    - m为整数，则$a \equiv b \pmod{m} \Leftrightarrow \exists k \in \mathbb{Z}\ \text{s.t.}\ a = b + km$
    - $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m}$
      $\rightarrow a + c \equiv b + d \pmod{m} \wedge ac \equiv bd \pmod{m}$

例

- 计算下列各式中的x
  - $20846 + 24268 - 42602 \equiv x \pmod{10}$
    - $0 \leq x \leq 9$
  - $26 \times 93 \times 12 \times 40 \equiv x \pmod{7}$
    - $0 \leq x \leq 6$
  - $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m}$
    $\rightarrow a + c \equiv b + d \pmod{m} \wedge ac \equiv bd \pmod{m}$

模算术

- 同余 (congruence)
  - $a, b \in \mathbb{Z}$，$m \in \mathbb{Z}^+$，若$m|(a-b)$，则称a模m同余b (a is congruent to b modulo m)
  - 记作$a \equiv b \pmod{m}$
  - 同余的性质
    - m为整数，则$a \equiv b \pmod{m} \Leftrightarrow \exists k \in \mathbb{Z}\ \text{s.t.}\ a = b + km$
    - $a \equiv b \pmod{m} \wedge c \equiv d \pmod{m}$
      $\rightarrow a + c \equiv b + d \pmod{m} \wedge ac \equiv bd \pmod{m}$
    - 同余式两侧同乘、加一个整数仍成立，除以不成立

模m算术

- 模m算术 (arithmetic modulo m)
  - 定义在$\mathbb{Z}_m = \{0,1,\ldots,m-1\}$上的算术
  - 加法
    - $a +_m b = (a + b) \bmod m$
    - 即a+b除以m的余数
  - 乘法
    - $a \cdot_m b = (a \cdot b) \bmod m$

例

- 计算
  - $7 +_{11} 9$
  - $7 \cdot_{11} 9$

- 加法
  - $a +_m b = (a + b) \bmod m$
- 乘法
  - $a \cdot_m b = (a \cdot b) \bmod m$

大纲

- 整除和模
- 整数表示和算法 (4.2)
- 素数和最大公约数
- 同余方程
- 同余的应用
- 密码学

整数的表示

- 现实中常用十进制
  - 10称为基数 (base)
  - 逢十进一
  - $965 = 9 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0$

整数的表示

- 现实中常用十进制
  - 10称为基数 (base)
  - 逢十进一
  - $965 = 9 \cdot 10^2 + 6 \cdot 10^1 + 5 \cdot 10^0$

- 其他基数
  - 2：二进制 (binary)
  - 8：八进制 (octal)
  - 16：十六进制 (hexadecimal)
  - 古玛雅用20进制，古巴比伦用60进制

整数的表示

- 表示的唯一性
  - 令b是一个大于1的整数，则$n \in \mathbb{Z}^+$可以唯一地表示为下面的形式

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$$

其中$k \in \mathbb{N}$，$a_i \in \mathbb{Z}_b$，且$a_k \neq 0$

整数的表示

- 表示的唯一性
  - 令b是一个大于1的整数，则$n \in \mathbb{Z}^+$可以唯一地表示为下面的形式

$$n = a_k b^k + a_{k-1} b^{k-1} + \ldots + a_1 b + a_0$$

其中$k \in \mathbb{N}$，$a_i \in \mathbb{Z}_b$，且$a_k \neq 0$

  - 该表示是n的b进制展开式 (base b expansion of n)
  - 记作$(a_k a_{k-1} \ldots a_1 a_0)_b$
  - 默认$b = 10$

b进制

- 二进制 (binary)
  - 0, 1
  - 用于计算机内运算
- 八进制 (octal)
  - 0,1,2,3,4,5,6,7
- 十六进制 (hexadecimal)
  - 0,1,2,3,4,5,6,7,8,9,A,B,C,D,E,F

b进制转十进制

- 给定$(a_k a_{k-1} \ldots a_1 a_0)_b$，求其十进制表示

- 十进制表示：

$$a_k b^k + a_{k\text{-}1} b^{k\text{-}1} + \ldots + a_1 b + a_0$$

例

- 计算下列各数的十进制表示
  - $(1\ 0101\ 1111)_2$
  - $(111)_8$
  - $(\mathrm{ABC})_{16}$

十进制转b进制

- 给定十进制数n，求其b进制表示

- 转换思路
  - n除以b的余数是其b进制的最后一位
  - 对商重复上述步骤

例

- 计算326的十六进制、八进制、二进制表示

十进制转b进制

procedure *base b expansion*(n, b: positive integers with b > 1)
$q := n$
$k := 0$
while ($q \neq 0$)
    $a_k := q$ **mod** b
    $q := q$ **div** b
    $k := k + 1$
return(a_{k-1},..., a_1,a_0){$(a_{k-1} \ldots a_1 a_0)_b$ is base b expansion of n}

q mod b是q除以b的余数
q div b 是q除以b的商

二、八、十六进制间转换

- 计算$(37274)_8$的十六进制表示

- 快速转换
  - 十六进制数字对应4个二进制数字
  - 八进制数字对应3个二进制数字

TABLE 1 Hexadecimal, Octal, and Binary Representation of the Integers 0 through 15.

Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Octal	0	1	2	3	4	5	6	7	10	11	12	13	14	15	16	17
Binary	0	1	10	11	100	101	110	111	1000	1001	1010	1011	1100	1101	1110	1111

快速模幂算法

- 计算$27^{13} \bmod 12$
  - 将指数13用二进制展开
  - 按i从小到大计算$27^i \bmod 12$
  - 将二进制展开中出现的项加起来

procedure *modular exponentiation*(*b*: integer, $n = (a_{k-1}a_{k-2}\ldots a_1a_0)_2$, *m*: positive integers)
x := 1
power := *b* **mod** *m*
for *i* := 0 to $k-1$
    if $a_i = 1$ **then** *x* := (*x*·*power*) **mod** *m*
    power := (*power*·*power*) **mod** *m*
return *x* {*x* equals b^n **mod** *m* }

大纲

- 整除和模
- 整数表示和算法
- 素数和最大公约数 (4.3)
- 同余方程
- 同余的应用
- 密码学

素数

- 素数 (prime)
  - p为大于1的整数，若p的正因子只有1和p，则称p为素数
  - 大于1的非素数称为合数 (composite)

  - 7是素数
  - 9=3*3是合数

素数

- 算术基本定理 (fundamental theorem of arithmetic)
  - 每个合数都可以唯一地写成两个或多个素数的乘积，其中素数因子以非递减序排列
  - 该写法是整数的素因子分解 (prime factorization)

例

- 给出下列各数的素因子分解
  - 100
  - 17
  - 126

筛法

- 埃拉托斯特尼筛法 (Sieve of Eratosthenes)
  - Eratosthenes：古希腊数学家 (276-194 B.C.)
  - 筛法可用于寻找小于某个数的所有素数
  - 筛去所有
    - 2以外所有2的倍数
    - 3以外所有3的倍数
    - 5以外所有5的倍数
    - ……
    - 直到不超过$\sqrt{n}$的素数为止

素数的性质

- 存在无限多个素数

素数的性质

- 存在无限多个素数
- $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$
  - $\pi(x)$ = 不超过x的素数个数

TABLE 2 Approximating $\pi(x)$ by $x/\ln x$.

x	$\pi(x)$	$x/\ln x$	$\pi(x)/(x/\ln x)$
10^3	168	144.8	1.161
10^4	1229	1085.7	1.132
10^5	9592	8685.9	1.104
10^6	78,498	72,382.4	1.084
10^7	664,579	620,420.7	1.071
10^8	5,761,455	5,428,681.0	1.061
10^9	50,847,534	48,254,942.4	1.054
10^{10}	455,052,512	434,294,481.9	1.048

素数的性质

- 存在无限多个素数
- $\lim_{x\to\infty}\frac{\pi(x)}{x/\ln x}=1$
- a,b互质时，形如$ak+b,k\in\mathbb{N}^+$的素数有无穷多个
  - 有无穷多个素数对应于$2k+1$型
  - $4k+3$型可类似证明

素数的性质

- 存在无限多个素数
- $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln x} = 1$
- a, b互质时，形如$ak + b, k \in \mathbb{N}^+$的素数有无穷多个
- $\forall n \in \mathbb{N}^+$，$\exists a, b \in \mathbb{N}^+$，使得$ak + b, 1 \le k \le n$均为素数
  - $n = 5$：$5, 11, 17, 23, 29$
  - 2006年由Ben Green和Terrence Tau (陶哲轩) 证明

素数的公开问题

- 生成大素数
  - 至今没有找到简单函数$f(n)$，使得$f(n)$均为素数
  - $f(n) = n^2 - n + 41$对1~40均为素数，但41不是
  - 整系数多项式无法满足$f(n)$均为素数

素数的公开问题

- 生成大素数
  - 至今没有找到简单函数$f(n)$，使得$f(n)$均为素数
- 哥德巴赫猜想
  - 每个大于2的偶数是两个素数之和
  - 陈景润1996年证明每个充分大的正偶数都可以写成如下两种形式之一
    - 两个素数之和
    - 一个素数以及两个素数乘积之和

素数的公开问题

- 生成大素数
  - 至今没有找到简单函数$f(n)$，使得$f(n)$均为素数
- 哥德巴赫猜想
  - 每个大于2的偶数是两个素数之和
- 孪生素数猜想
  - 形如$(p, p+2)$的素数对有无穷多对
  - 张益唐2013年证明了存在无穷多对差距小于7kw的素数对

最大公约数

- 最大公约数 (greatest common divisor)
  - a, b是不全为零的整数，满足$d|a$且$d|b$的最大整数d称为a和b的最大公约数
  - 记作$\gcd(a, b)$
  - 例
    - 使用质因数分解计算gcd(120,500)
    - 质因数分解没有高效算法

最大公约数

- 最大公约数 (greatest common divisor)
  - a, b是不全为零的整数，满足$d|a$且$d|b$的最大整数d称为a和b的最大公约数
  - 记作$\gcd(a, b)$

  - $\gcd(a, b) = 1$时，称a和b互质 (relatively prime)
  - 若$a_1, a_2, \ldots, a_n$满足$\gcd(a_i, a_j) = 1, (i \neq j)$，则称它们两两互质 (pairwise relatively prime)

例

- 判断下列每组数是否两两互质
  - 10, 17, 21
  - 10, 19, 24

最大公约数

- 性质
  - 令 $a = bq + r$，其中，a, b, q, r 为整数，则

$$\gcd(a,b) = \gcd(b,r)$$

例

- 利用下列性质计算gcd(120,500)

令 $a = bq + r$，其中，a, b, q, r 为整数，则

$$\gcd(a,b) = \gcd(b,r)$$

最大公约数

- 性质
  - 令 $a = bq + r$，其中，a, b, q, r 为整数，则

$$\gcd(a,b) = \gcd(b,r)$$

- 欧几里得算法

```
procedure gcd(a, b: positive integers)
x := a
y := b
while   y ≠ 0
        r := x mod y
        x := y
        y := r
return x {gcd(a,b) is x}
```

最小公倍数

- 最小公倍数 (least common multiple)
  - $a, b \in \mathbb{Z}^+$，满足$a|n$且$b|n$的最小n称作a和b的最小公倍数
  - 记作$\mathrm{lcm}(a, b)$

最小公倍数

- 最小公倍数 (least common multiple)
  - $a, b \in \mathbb{Z}^+$，满足$a|n$且$b|n$的最小n称作a和b的最小公倍数
  - 记作$\text{lcm}(a, b)$

- 若a,b为正整数，则 $ab = \gcd(a,b) \cdot \text{lcm}(a,b)$

例

- 计算gcd(91,287)和lcm(91,287)

同余式除法

- 下列两式通常不等价
  - $ac \equiv bc \pmod{m}$
  - $a \equiv b \pmod{m}$

- 当$\gcd(c, m) = 1$时等价
  - $ac \equiv bc \pmod{m} \wedge \gcd(c, m) = 1$
    $\Rightarrow a \equiv b \pmod{m}$

总结

- 整除和模
  - 整除、因子、同余、模算数
- 整数表示和算法
  - 二、八、十六进制与十进制间转换
  - 二、八、十六进制间快速转换
  - 快速模幂算法
- 素数和最大公约数
  - 素数的概念、筛法、无限性
  - 算术基本定理（质因数分解）
  - 最大公约数、最小公倍数、互质、欧几里得算法