第十四讲 有关数论算法

内容提要：

- 初等数论概念
- 最大公约数
- 模运算和模线性方程
- 中国余数定理

初等数论概念

◻ 整除性和约数

1）d | a ，读作”d整除a”，表示a是d的倍数；

2）**约数**：d | a 且d>0，则d是a的约数；（即定义约数为非负整数）

3）对整数a最小约数为1，最大为|a|。其中，1和|a|为整数的平凡约数,而a的非平凡约数称为a的因子；

◻ 素数和合数

1) 素数(质数)：对于整数a > 1，如果它仅有平凡约数1和a，则a为素数；

2) 合数：不是素数的整数a ，且 a > 1;

3) 整数1被称为基数，它不是素数也不是合数；

4) 整数0和所有负整数既不是素数也不是合数；

初等数论概念

- 已知一个整数n，所有整数都可以划分为是n的倍数的整数，以及不是n的倍数的整数。对于不是n的倍数的那些整数，又可以根据它们除以n所得的余数来进行分类。——数论的大部分理论都是基于这种划分
- **除法定理（Th31.1）：**

> 对任何整数a和正整数n，存在唯一整数q和r，使得 $a=qn+r$，这里 $q=\lfloor a/n \rfloor$，$0 \le r < n$。

其中，q为商，值r = a mod n称为余数。

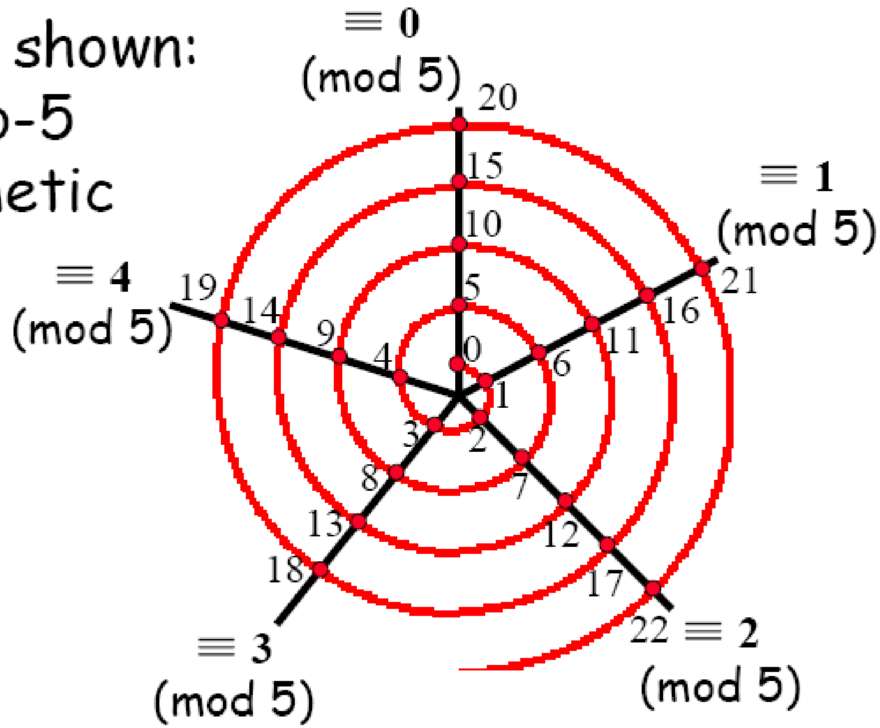
- 根据整数模n所得的余数，可以把整数分为n个等价类。包含整数a的模n等价类为：$[a]_n = \{ a + nk \mid k \in Z \}$。如 $[3]_7 = \{\ldots, -4, 3, 10, 17, \ldots\}$

  模n等价类可以用其最小非负元素来表示，如3表示$[3]_7$
- 性质：如果 $a \in [b]_n$，则 $a \equiv b \pmod{n}$

初等数论概念

- **Spiral Visualization of mod:**

Example shown:
modulo-5
arithmetic



初等数论概念

- **公约数**：d是a的约数也是b的约数，则d是a和b的公约数。
- **公约数性质**：

  -- $d \mid a$且$d \mid b$蕴含着$d \mid (a+b)$和$d \mid (a-b)$

  -- 对任意整数x和y，有 $d \mid a$ 且 $d \mid b$ 蕴含着 $d \mid (ax + by)$

  -- 如果$a \mid b$ 则 $|a| \le |b|$或者$b=0$, 这说明 "$a|b$且$b|a$，则$a = +/- b$"

- **最大公约数**：

  -- gcd(a, b)表示两个不同时为0的整数a和b的最大公约数；

  -- gcd(a,b)介于1和min(|a|, |b|) 之间；

- **gcd基本性质**：

  -- $\gcd(a, 0) = |a|$;

  -- $\gcd(a, ka) = |a|$;

初等数论概念

最大公约数性质：

- **Th31.2**

  a, b为不全为零的两个整数，则最大公约数gcd(a, b)是 $\{ax+by \mid x,y \in Z\}$中最小的正整数。

  -系1：对所有整数a和b，如果d|a，d|b，则d|gcd(a, b)

  -系2：对所有整数a和b，和非负整数n，有

  $$\gcd(an, bn) = n\gcd(a, b)$$

  -系3：对所有正整数n、a和b，如果n|ab且gcd(a, n)=1，则 n|b

初等数论概念

- **互质数：** 如果gcd(a,b)=1,则称a与b为互质数；
- 如果两个整数中每一个数都与一个整数p互为质数，则它们的积与p互为质数，即：

> **Th31.6**
>
> $\forall a, b, p \in Z$，如果gcd(a, p)=1和gcd(b, p)=1，则 gcd(ab, p)=1

- **唯一因子分解：**

> **定理31.7:** 对所有素数p和所有整数a, b, 如果 $p \mid ab$，则 $p \mid a$ 或 $p \mid b$（或者两者都成立）

> **Th31.8(唯一分解定理)**
>
> 一个合数a能被唯一写成形式 $a=p_1^{e_1}p_2^{e_2}\dots p_r^{e_r}$
>
> 这里p_i是素数，$p_1 < p_2 < \dots < p_r$，e_i是正整数
>
> 如，$6000=2^4 \times 3 \times 5^3$

最大公约数

- 一种直观求解GCD：

  根据a和b的素数因子分解，求出正整数a和b的最大公约数gcd(a,b)，即：

$$a = p_1^{e1} p_2^{e2} \dots p_r^{er} \text{ 和 } b = p_1^{f1} p_2^{f2} \dots p_r^{fr}$$
$$\Rightarrow gcd(a, b) = p_1^{\min(e1, f1)} p_2^{\min(e2, f2)} \dots p_r^{\min(er, fr)}$$

注：这种解法需要整数的素因子分解，而素因子分解是一个很难的问题（NP问题）

最大公约数

欧几里得算法

- Th.31.9（GCD递归定理）：对任何非负整数a和正整数b，有gcd(a,b) = gcd(b, a mod b)；

* 可以通过证明gcd(a,b)=+/- gcd(b, a mod b)来证明该定理！见P526

- 伪代码：

```
Euclid(a, b)
{
    if  b=0 then
            return a;
    else
            return  Euclid(b, a mod b);
}
```

例子：

Euclid(30, 21)
= Euclid (21, 9)
= Euclid (9, 3)
= Euclid (3, 0)

最大公约数

□ Euclid算法的运行时间：

- **Th.31.11(拉姆定理)**

  对整数$k \geq 1$，如果$a>b \geq 1$且$b<F_{k+1}$，

  则Euclid(a, b)递归调用的次数小于k。

注：

- Euclid's Alg.递归调用的次数为$O(\log b)$
- 算法应用到二个β位整数上，
  算法耗费$O(\beta)$算术运算和
  $O(\beta^3)$位运算

Gabriel Lamé
1795-1870

最大公约数

扩展的Euclid算法：

- 问题

  Find x, y s.t. gcd(a, b) =ax+by

- 算法

```
ExtendedEuclid(a, b)
{  if b=0 then
       return (a, 1, 0);
   (d′, x′, y′) ← EctendedEuclid(b, a mod b);
   (d, x, y) ← (d′, y′, x′-⌊a/b⌋y′);
   return (d, x, y);
}
```

- 例：把3=gcd(99, 78)表示成99和78的线性组合

最大公约数

- 用计算gcd(99, 78)的例子说明Extended-Euclid的执行过程:

a	b	floor(a/b)	d	x	y
99	78	1	3	-11	14
78	21	3	3	3	-11
21	15	1	3	-2	3
15	6	2	3	1	-2
6	3	2	3	0	1
3	0	-	3	1	0

$$\begin{cases} \gcd(a,b) = \gcd(b, a \bmod b) \\ \gcd(a,0) = a \end{cases} \Longrightarrow (d, x, y) = (a, 1, 0)$$

$$\begin{cases} x = y' \\ y = x' - \lfloor a/b \rfloor y' \end{cases}$$

模运算和模线性方程

- 群(S, ⊕)是一个集合S和定义在S上的二进制运算⊕，且满足封闭性、单位元、结合律、逆元等4个性质；
- 交换群（a ⊕ b = b ⊕ a）和有限群：
  - **Def. 1:**

    设Z_n={ $[a]_n$ | 0≤ a ≤n-1}, 定义加法运算$+_n$:

    $[a]_n +_n [b]_n = [a+b]_n$,

    则(Z_n, $+_n$)是有限Abelian群

    如, (Z_6, $+_n$), Z_6 ={$[0]_6$, $[1]_6$, $[2]_6$, $[3]_6$, $[4]_6$, $[5]_6$}

  - **Def. 2:**

    设Z_n^*={ $[a]_n \in Z_n$ | gcd(a, n)=1 }, 定义乘法运算$\times_n$:

    $[a]_n \times_n [b]_n = [a \times b]_n$,

    则(Z_n^*, $\times_n$)是有限Abelian群

    如, (Z_{15}^*, $\times_n$), Z_6^* ={1, 2, 4, 7, 8, 11, 13, 14}

模运算和模线性方程

- **Theorem(Euclid's phi Func.)**

  令$\phi(n)$为Z_n^*的size，则有$\phi(n) = n\prod_{p|n}(1-\frac{1}{p})$

- 例：

  $Z_{15}^* = \{1, 2, 4, 7, 8, 11, 13, 14\}$

  $|Z_{15}^*| = 15(1-1/3)(1-1/5) = 8$

- 其中，p包括能整除n的所有素数（如果n是素数，则也包括n本身）
- 直观上看，开始时有一张n个余数组成的表{0,1,···,n-1}，然后对每个能整除n的素数p，在表中划掉所有是p的倍数的数。
- 如果p是素数，则$Zp^*=\{1,2,\cdots,p-1\}$，并且$\Phi(p) = p-1$
- 如果n是合数，则$\Phi(n)<n-1$

模运算和模线性方程

- **子群：** 如果(S, ⊕)是一个群，S′ 是S的一个子集，并且（S′，⊕) 也是一个群，则(S′，⊕)称为(S, ⊕)的子群。

- 下面定理对子群规模作出了一个非常有用的限制：
  - **Th. 31.15 (Lagrange's Theorem)**

    如果H是有限群G的子群，那么$|H|$整除$|G|$

    系：$|H| \le |G|/2$

模运算和模线性方程

□ 由一个元素生成的子群：

从有限群(S, ⊕)中，选取一个元素a，并取出根据群上的运算由a所能生成的所有元素，这些元素构成了原有限群的一个子群。

$$a^{(k)} = \bigoplus_{i=1}^{k} a = \underbrace{a \oplus a \oplus \cdots \oplus a}_{k}$$

- * 在群 Z_n 中，有$a^{(k)} = ka \bmod n$;
- * 在群Z_n^*中，有$a^{(k)} = a^k \bmod n$;

□ 由a生成的子群用<a>或者(<a>,⊕)来表示，其定义如下：

$$\langle a\rangle = \{ a^{(k)} : k \geq 1 \}$$

称为 a 生成子群<a>或者a是<a>的生成元。

模运算和模线性方程

- **问题描述：**

求x满足下面模方程：

$$ax \equiv b \pmod{n}$$

这里 $a > 0$， $n > 0$

模运算和模线性方程

$\langle a \rangle$群表示和构造定理

- **Def.:**

  令$\langle a \rangle$是Z_n上由a生成的子群，$\langle a \rangle=\{\, ax \bmod n \mid x\geq 0, x\in Z\}$

- 性质：

  方程$ax \equiv b \pmod{n}$有解 $\Leftrightarrow b\in\langle a \rangle$

- **Th31.20(构造定理)**

  对正整数a和n，$d=\gcd(a, n)$，则有

  $\langle a \rangle = \langle d \rangle = \{\, 0, d, 2d, \ldots, (n/d - 1)d \,\}$

  为Z_n上子群，且$|\langle a \rangle| = n/d$

模运算和模线性方程

- **推论1：** 方程 $ax \equiv b \pmod{n}$ 对于未知量x有解，当且仅当 $\gcd(a, n) \mid b$。
- **推论2：** 方程 $ax \equiv b \pmod{n}$ 或者对模n有d个不同的解，其中 $d = \gcd(a, n)$，或者无解。

模运算和模线性方程

- 例：判断$4x \equiv 2 \pmod 6$ 和 $4x \equiv 3 \pmod 6$有无解

$\because \gcd(4, 6) | 2 \quad \therefore 4x \equiv 2 \pmod 6$有解

$\because \gcd(4, 6)$不整除3 $\quad \therefore 4x \equiv 3 \pmod 6$无解

注：

i:	0	1	2	3	4	5
<4>: 4i mod 6 =	0	4	2	0	4	2

可以看出：第一个方程有二个解2，5；

第二个方程无解

模运算和模线性方程

- 输入a和n为任意正整数，b为任意整数

Modular-Linear-Equation-Solver(a, b, n)

{

  (d', x', y') ← Extended-Euclid(a, n);

  if d | b

    then x_0 ← x'(b/d) mod n

      for i ← 0 to d-1

        do printf (x_0+i(n/d)) mod n

    else print "no solutions"

}

模运算和模线性方程

求解方法：

- 先求特解
  - Th31.23 设d=gcd(a, n)且d=ax'+ny'，对某个整数x'和y'。
    如果d|b，则有特解$x_0 = x'(b/d) \bmod n$

  证：

$$
\begin{aligned}
ax_0 &\equiv ax'(b/d) \pmod n \\
&\equiv d(b/d) \pmod n \quad // \because ax'+ny'=d \quad \therefore ax' \equiv d \bmod n \\
&\equiv b \pmod n
\end{aligned}
$$

- 求全部解
  - Th31.24 设x_0为$ax \equiv b \pmod n$的一个解，则有d个不同解：

$$x_i \equiv x_0 + i(n/d) \quad i=0,1, \dots, d-1$$

模运算和模线性方程

- 示例：$14x \equiv 30 \pmod{100}$

解:

①调用ExtendedEuclid(14, 100) $\Rightarrow (d, x', y')=(2, -7, 1)$

② $\because\ 2|30$, $\therefore$ 特解$x_0 = -7 \times 30/2 \pmod{100} = 95$

③调用 求全部解算法：二个解95，45

$$x_0 = 95 + 0 \times 100/2 = 95$$

$$x_1 = 95 + 1 \times 100/2 = 145 \equiv 45 \pmod{100}$$

中国余数定理

- 中国余数定理，也称中国剩余定理，孙子剩余定理。
- 从《孙子算经》到秦九韶《数书九章》对一次同余式问题的研究成果，在19世纪中期开始受到西方数学界的重视。1852年，英国传教士伟烈亚力向欧洲介绍了《孙子算经》的“物不知数”题和秦九韶的“大衍求一术”；1876年，德国人马蒂生指出，中国的这一解法与西方19世纪高斯《算术探究》中关于一次同余式组的解法完全一致。从此，中国古代数学的这一创造逐渐受到世界学者的瞩目，并在西方数学史著作中正式被称为“中国剩余定理”。

中国余数定理

- **韩信点兵：**

韩信是汉高祖刘邦手下的大将，他英勇善战，智谋超群，为汉朝的建立了卓绝的功劳。据说韩信的数学水平也非常高超，他在点兵的时候，为了保住军事机密，不让敌人知道自己部队的实力，先令士兵从1至3报数，然后记下最后一个士兵所报之数；再令士兵从1至5报数，也记下最后一个士兵所报之数；最后令士兵从1至7报数，又记下最后一个士兵所报之数；这样，他很快就算出了自己部队士兵的总人数，而敌人则始终无法弄清他的部队究竟有多少名士兵。

这个故事中所说的韩信点兵的计算方法，就是现在被称为“中国剩余定理”的一次同余式解法。它是中国古代数学家的一项重大创造，在世界数学史上具有重要的地位。

中国余数定理

- 最早提出并记叙这个数学问题的，是南北朝时期的数学著作《孙子算经》中的“物不知数”题目。这道“物不知数”的题目是这样的：

> “今有一些物不知其数量。如果三个三个地去数它，则最后还剩二个；如果五个五个地去数它，则最后还剩三个；如果七个七个地去数它，则最后也剩二个。问：这些物一共有多少？”

- 用数学语言来表述就是如下线性同余方程

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 3 \pmod 5 \\ x \equiv 2 \pmod 7 \end{cases}$$

《孙子算经》实际上是给出了这类一次同余式组 的一般解：

中国余数定理

- 但由于题目比较简单，甚至用试猜的方法也能求得，所以《孙子算经》尚没有上升到一套完整的计算程序和理论的高度。

- 真正从完整的计算程序和理论上解决这个问题的，是南宋时期的数学家秦九韶。秦九韶在他的《数书九章》中提出了一个数学方法“大衍求一术”，系统地论述了一次同余式组解法的基本原理和一般程序。

- 如今，中国余数定理广泛应用于通信领域。譬如，电子工程师发明的“中国余数码”(Chinese Remainder Code) 是一种常用的纠错编码 (error correcting code)。

中国余数定理

- **定理31.24:** 假设方程 $ax \equiv b \pmod{n}$有解（即有gcd(a,n)|b），x_0是方程的任意一个解，则该方程对模n恰有d个不同的解，分别为：

$$x_i = x_0 + i(n/d) \qquad (\ i = 1, 2, \ldots, d\text{-}1\ )$$

- **推论31.25:**

  对任意n > 1, 如果gcd(a, n) = 1，则方程 ax ≡ b (mod n)对模n有唯一解。

- **推论31.26:**

  对任意n > 1, 如果gcd(a, n) = 1，则方程 ax ≡ 1 (mod n)对模n有唯一解，否则无解。

  - ✓ 所求得的解x是a对模n乘法的逆元，并用记号(a^{-1} mod n)来表示；
  - ✓ 如果gcd(a,n)=1，则方程ax ≡ 1 (mod n)的一个解就是EXTENDED-EUCLID所返回的整数x；

中国余数定理

a 模n的逆存在唯一性定理:

- **Def.** :

  若x使得 $xa \equiv 1 \pmod{n}$，称x为a模n的逆

- **Theorem:**

  若a和n互素，n>1，则唯一存在a模n的逆。

  注:

  - 以下记a模n的逆为a^{-1}，使$a^{-1}a \equiv 1 \pmod{n}$
  - 本定理实际上给出了求a模n的逆的方法

- 例：(1)求3模7的逆；　(2)求$3x \equiv 4 \pmod{7}$

中国余数定理

- CRT(China Remainder Theorem)

  令$n_1, n_2, \ldots, n_k$为两两互素的正整数，则同余方程组

  $$x \equiv a_1 \pmod{n_1}$$
  $$x \equiv a_2 \pmod{n_2}$$
  $$\ldots$$
  $$x \equiv a_k \pmod{n_k}$$

  有唯一的模$n= n_1n_2 \ldots n_k$解x。

  注：本定理实际上给出了求解方法

- 例(一个中国古代问题)

谢谢！

Q & A