PART 3

数论基础

目录 CONTENTS

3.1 整除性和带余除法

序言

- 数论是研究整数性质的一门很古老的数学分支，其初等部分是以整数的整除性为中心的，包括整除性、不定方程、同余式、连分数、素数（即质数）分布 以及数论函数等内容，统称初等数论（**elementary number theory).**
- 初等数论是数论中不求助于其他数学学科的帮助，只依靠初等的方法来研究整数性质的分支.
- 数论是是密码学的基础,主要应用于古典密码学、公钥密码学等知识领域.

3.1整除性和带余除法

整除性

定义　设 a,b 是任意两个整数，其中 $b\neq 0$,

如果存在一个整数 m 使得 等式

$$a=bm \qquad (1)$$

成立，我们就说 b 整除 a 或 a 可被 b 整除, 记作 $b\mid a$,

此时我们把 b 叫作 a 的因数, 把 a 叫作 b 的倍数.

如果(1)里的整数 m 不存在,我们就说 b 不能 整除 a

或 a 不被 b 整除, 记作 $b\nmid a$.

3.1整除性和带余除法

整除性

- 例：24的正因子是1,2,3,4,6,8,12,24.

$$13 \mid 182 \Leftrightarrow 182 = 13 \times 14$$

$$-5 \mid 30 \Leftrightarrow 30 = (-5) \times (-6)$$

$$17 \mid 289 \Leftrightarrow 289 = 17 \times 17$$

$$-3 \mid 33 \Leftrightarrow 33 = (-3) \times 11$$

$$17 \mid 0 \Leftrightarrow 0 = 17 \times 0$$

$$2 \nmid 7 \Leftrightarrow 7 = 3 \times 2 + 1$$

注意：整除和除法的区别

整除性

Proposition.

Let $a,\ b, c$ be integers, $a \neq 0, b \neq 0$. Then

(i) If $a \mid 1$, then $a = \pm 1$.

(ii) If $a \mid b$, and $b \mid a$, then $a = \pm b$.

(iii) Any $b \neq 0$ divies 0.

(iv)** If $a \mid b$ and $b \mid c$, then $a \mid c$

整除性

Proposition.

(iv) Proof: Because $a \mid b$ and $b \mid c$, there are integers e and f such that $ae = b$ and $bf = c$. Hence, $c = bf = (ae)f = a(ef)$, and we conclude that $a \mid c$.

Example

Because $11 \mid 66$ and $66 \mid 198$, Proposition (iv) tells us that $11 \mid 198$.

整除性

Proposition.

If $b \mid g$ and $b \mid h$, then $b \mid (mg + nh)$ for arbitrary integers m and n.

Proof: Because $b \mid g$ and $b \mid h$, there are integers g_1 and h_1 such that $g = b \times g_1$ and $h = b \times h_1$.

Hence, $mg + nh = mbg_1 + nbh_1 = b(mg_1 + nh_1)$.

Consequently, we see that $b \mid mg + nh$.

整除性

例： $b=7, g=14, h=63, m=3, n=2$

因为 $7 \mid 14, 7 \mid 63$，所以 $7 \mid (3\times 14+2\times 63)$，

我们有 $(3\times 14+2\times 63)=7(3\times 2+2\times 9)$，

显然 $7 \mid 7(3\times 2+2\times 9)$.

整除性

例 证明：若 $3 \mid n$ 且 $7 \mid n$，则 $21 \mid n$.

由 $3 \mid n$ 知 $n = 3m$, 所以 $7 \mid 3m$. 由此及 $7 \mid 7m$

得 $7 \mid (7m - 2 \cdot 3m) = m$. 因而有 $21 \mid n$.

带余除法

定理 带余数除法

若 a,n是两个整数,其中 $b>0$, 则存在着两个整数q及r,使得

$$a=nq+r,\quad 0\le r<n;q=\lfloor a/n\rfloor$$

成立,而且q及r 是惟一的.

带余除法

证明思路:

存在性: 构造序列$\cdots$，$-3n,-2n,-n,0,n,2n,3n,\cdots$

惟一性：设还有两个整数q_1与r_1满足

$a=nq_1+r_1,0\le r_1<n$.只要证明$r_1=r,q_1=q$即可.

带余除法

证　存在性　做整数序列

$$\cdots,-3n,-2n,-n,0,n,2n,3n,\cdots$$

则a必在上述序列的某两项之间，

即存在一个整数q使得

$$qn \le a < (q+1)n$$

成立. 令 $a-nq=r$,则$a=nq+r$,而$0 \le r < n$.

带余除法

证 唯一性 设 q_1, r_1 是满足等式的两个整数,则

$$a = nq_1 + r_1, 0 \le r_1 < n,$$

因而 $nq_1 + r_1 = nq + r,$

于是 $n(q - q_1) = r_1 - r,$

故 $n|q - q_1| = |r_1 - r|,$

由于 r 及 r_1 都是小于 n 的整数,所以上式右边是小于 n 的. 如果 $q \neq q_1$ 则上式左边 $\ge n$. 这是不可能的.

因此 $q = q_1$ 而 $r = r_1$.

3.1整除性和带余除法

带余除法

定义 $a=nq+r,0\le r<n$中的q叫做a被b除所得的不完全商,r叫做a被n除所得到的余数.

例 设$n=15$,则 当$a=255$时

$a=17n+0,r=0<15$,而$q=17$;

当$a=417$时，$a=27n+12,0<r=12<15$,而$q=27$;

当$a=-81$时，$a=-6n+9,0<r=9<15$,而$q=-6$.

3.1整除性和带余除法

带余除法的内涵

- 它可以看作是整除的推广，也可以用带余除法定理来定义整除性
- 将一个未知的整数表示为小于除数的余数，将整数进行分类，从而可将无限问题转化为有限问题
- 其他应用：辗转相除法、进制间转换算法

3.1整除性和带余除法

带余除法的的应用：整数分类

- 整数分类的依据：根据带余数除法可以进一步

  根据 r 的取值范围定义

3.1整除性和带余除法

带余除法的的应用：整数分类

推论　设 $a>0$.任一整数被 a 整除后所得的最小非负余数是且仅是 $0, 1, \cdots, a-1$ 这 a 个数中的一个.

例:设$a \geq 2$是给定的正整数，j=0, 1, $\cdots$, $a-1$.对给定的 j, 被 a 除后余数等于 j 的全体整数是 $ka+j, k=0, \pm 1, \pm 2, \ldots$. 这些整数组成的集合记为 $j \bmod a$. 当$0 \leq j \neq j' \leq a-1$时 $j \bmod a$ 集合和 $j' \bmod a$ 不相交,以及并集

$$0 \bmod a \cup 1 \bmod a \cup \cdots \cup (a-1) \bmod a = Z,$$

即全体整数被 a 除后所得的最小非负余数来分类,分为了两两不相交的 a 个类.

3.1整除性和带余除法

带余除法的的应用：整数分类

例 $a=2$ 时，全体整数分为两类：

$$0 \bmod 2=\{2k : k \in Z\}, 1 \bmod 2=\{2k+1 : k \in Z\};$$

$a=3$ 时，全体整数分为三类：

$$0 \bmod 3=\{3k : k \in Z\}, 1 \bmod 3=\{3k+1 : k \in Z\},$$

$$2 \bmod 3=\{3k+2 : k \in Z\};$$

$a=6$ 时，全体整数分为六类：

$$0 \bmod 6=\{6k : k \in Z\}, 1 \bmod 6=\{6k+1 : k \in Z\},$$

$$2 \bmod 6=\{6k+2 : k \in Z\}, 3 \bmod 6=\{6k+3 : k \in Z\},$$

$$4 \bmod 6=\{6k+4 : k \in Z\}, 5 \bmod 6=\{6k+5 : k \in Z\};$$

3.2 欧几里得算法

3.2欧几里得算法

设a,b是任意两个正整数,由带余数除法,我们有下面的系列等式:

$$a = bq_1 + r_1, \quad 0 < r_1 < b,$$

$$b = r_1q_2 + r_2, \quad 0 < r_2 < r_1,$$

$$r_1 = r_2q_3 + r_3, \quad 0 < r_3 < r_1,$$

$$\cdots\cdots\cdots$$

$$r_{n-2} = r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1},$$

$$r_{n-1} = r_nq_{n+1} + r_{n+1}, r_{n+1} = 0,$$

$$d = \gcd(a,b) = r_n$$

3.2欧几里得算法

因为每进行一次带余数除法,余数就至少减一,而b是有限的,所以我们最多进行b次带余数除法,总可以得到一个余数是零的等式,即$r_{n+1}=0$.(2.3)式所指的计算方法,叫作辗转相除法.在西方常把它叫做欧几里得除法.它就是我国著名的古代数学著作《九章算术》中提出的“更相减损术”.

3.2欧几里得算法

定理：对任意非负整数 a 和正整数 b，有

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

证明：假设 $a>b$，根据带余除法，可将 a 表示为 $a=kb+r$，所以 $r=a-kb$。

设 d 是 a，b 的公因子，即 $d|a$，$d|b$，所以 $d|kb$。由 $d|a$ 和 $d|kb$ 得 $d|(a-kb)$，因此 d 是 b 和$(a-kb)$ 的公因子。

所以得出 a，b 的公因子集合与 b，$a \bmod b$ 的公因子集合相等，两个集合的最大值也相等。（证毕）

3.2欧几里得算法

✓ 在求两个数的最大公因子时，可重复使用以上结论。

例如：**gcd(55, 22) = gcd(22, 55 mod 22)**

= gcd(22,11)

= gcd(11, 0)

= 11。

gcd(18,12) = gcd(12,6) = gcd(6,0) = 6,

gcd(11,10) = gcd(10,1) = gcd(1,0) = 1。

3.2欧几里得算法

定理 若a,b是任意两个整数,则(a,b)就是

最后一个不等于零的余数,即 $(a,b)=r_n$.

证: $r_n=\gcd(0,r_n)=\gcd(r_{n+1},r_n)=\gcd(r_n,r_{n-1})$

$$=\cdots=\gcd(r_1,b)=\gcd(a,b)$$

$$a=bq_1+r_1,\quad 0<r_1<b,$$
$$b=r_1q_2+r_2,\quad 0<r_2<r_1,$$
$$r_1=r_2q_3+r_3,\quad 0<r_3<r_1,$$
$$\cdots\cdots$$
$$r_{n-2}=r_{n-1}q_n+r_n,\quad 0<r_n<r_{n-1},$$
$$r_{n-1}=r_nq_{n+1}+r_{n+1},r_{n+1}=0,$$
$$d=\gcd(a,b)=r_n$$

3.2欧几里得算法

例: 求gcd(1970, 1066)

- 1970=1×1066+904, gcd(1066, 904)
- 1066=1×904+162, gcd(904, 162)
- 904=5×162+94, gcd(162, 94)
- 162=1×94+68, gcd(94, 68)
- 94=1×68+26, gcd(68, 26)
- 68=2×26+16, gcd(26, 16)
- 26=1×16+10, gcd(16, 10)
- 16=1×10+6, gcd(10, 6)
- 10=1×6+4, gcd(6, 4)
- 6=1×4+2, gcd(4, 2)
- 4=2×2+0, gcd(2, 0)

因此gcd(1970, 1066)=2。

3.2欧几里得算法

例　求198和252的最大公约数.

$$252 = 1 \cdot 198 + 54$$

$$198 = 3 \cdot 54 + 36$$

$$54 = 1 \cdot 36 + 18$$

$$36 = 2 \cdot 18$$

3.2欧几里得算法

✓ **Euclid 算法描述：**

因 gcd(*a*, *b*)=gcd(|*a*|, |*b*|)，因此可假定算法的输入是两个正整数，设为 *a*，*b*，并设 *a*>*b*。

Euclid（*a*, *b*）

1. *X*←*a*; *Y*←*b*;

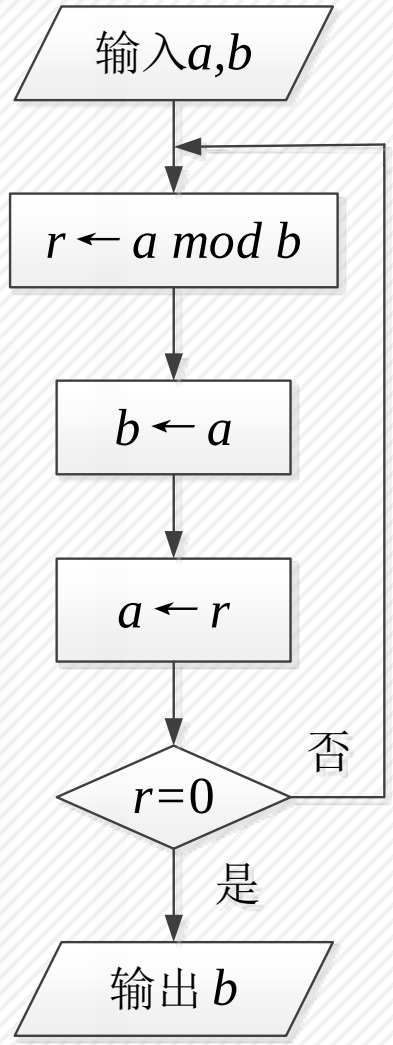
2. if *Y*=0 then return *X*=gcd(*a*, *b*);

3. *R*=*X* mod *Y*;

4. *X*=*Y*;

5. *Y*=*R*;

6. goto 2。



时间复杂性：O(log n)

扩展欧几里得算法

Finding u and v: $\gcd(a, b) = ua + vb$

- By back substitution from Euclidean Algorithm

$$
\begin{aligned}
a &= b \cdot q_1 + r_2 \\
b &= r_2 \cdot q_2 + r_3 \\
r_2 &= r_3 \cdot q_3 + r_4 \\
r_3 &= r_4 \cdot q_4 + r_5 \\
&\vdots \quad \vdots \\
r_{n-2} &= r_{n-1} \cdot q_{n-1} + \boxed{r_n} \\
r_{n-1} &= r_n \cdot q_n \\
\gcd(a,b) &= r_n
\end{aligned}
$$

$$
\begin{aligned}
r_n &= \gcd(a,b) \\
&= r_{n-2} - r_{n-1} \cdot q_{n-1} \\
&= r_{n-2} - \left(r_{n-3} - r_{n-2} \cdot q_{n-2}\right) \cdot q_{n-1} \\
&= r_{n-2}\left(1 + q_{n-2} \cdot q_{n-1}\right) - r_{n-3} \cdot q_{n-1} \\
&= \left(r_{n-4} - r_{n-3} \cdot q_{n-3}\right)\left(1 + q_{n-2} \cdot q_{n-1}\right) \\
&\quad - r_{n-3} \cdot q_{n-1} \\
&\cdots\cdots \\
&= ua + vb
\end{aligned}
$$

扩展欧几里得算法

例 求198和252的最大公约数，并把它表为198和252的整系数线性组合.

$$252 = 1\cdot 198 + 54$$
$$198 = 3\cdot 54 + 36$$
$$54 = 1\cdot 36 + 18$$
$$36 = 2\cdot 18$$

$$\begin{aligned} 18 &= -198 + 4(252 - 198) \\ &= 4\cdot 252 - 5\cdot 198 \\ 18 &= 54 - (198 - 3\cdot 54) \\ &= -198 + 4\cdot 54 \\ 18 &= 54 - 36 \end{aligned}$$

扩展欧几里得算法

例 设a= 963和b= 657，① 求最大公因数 gcd(a,b)；

②求整数s,t，使得$as+bt$ = gcd(a,b)。

解：利用欧几里德算法可得

$963 = 1\times657+306$　　$9 = 7\times657 - 15\times(963 - 657) = 22\times657 - 15\times963$

$657 = 2\times306+45$　　$9 = 7\times(657 - 2\times306) - 306 = 7\times657 - 15\times306$

$306 = 6\times45 +36$　↓↑　$9 = 45 - (306 - 6\times45) = 7\times45 - 306$

$45 = 1\times36 + 9$　　$9 = 45 - 36$

$36 = 4\times9$

于是

① 963和657的最大公因数 gcd(963,657)= 9；

② s= −15, t= 22，使得

$$963 \times (-15) + 657 \times 22 = \gcd(963,657) = 9$$

3.3 模运算

3.3模运算

- 设 n 是一正整数，a 是整数，如果用 n 除 a，得商为 q，余数为 r，则

$$a=qn+r,\ 0\leqslant r<n, \qquad q=\left\lfloor a/n \right\rfloor$$

其中$\lfloor x \rfloor$为小于或等于 x 的最大整数。

- 用 $a \bmod n$ 表示余数 r，则 $a=\left\lfloor a/n \right\rfloor n+a \bmod n$ 。
- 如果$(a \bmod n)=(b \bmod n)$，则称两整数 a 和 b 模 n 同余，记为 $a\equiv b \bmod n$。称与 a 模 n 同余的数的全体为 a 的同余类，记为$[a]$，称 a 为这个同余类的表示元素。
- 注意： 如果 $a\equiv 0 \pmod n$，则 $n|a$。

3.3模运算

例　　$11 \bmod 7=4$,　　$-11 \bmod 7=3$

例　$7 \equiv 2 \pmod 5$，$7 \not\equiv 9 \pmod 5$，$21 \equiv -9 \pmod{10}$

同余在日常生活中的应用

- 钟表对于小时是模12或24的，对于分钟和秒是模60的
- 日历对于星期是模7的，对于月份是模12的
- 电水表通常是模1000的
- 里程表通常是模100000的

3.3 模运算

同余的性质

✧ 同余有以下性质：

① 若 $n|(a-b)$，则 $a \equiv b \bmod n$。

② $(a \bmod n) \equiv (b \bmod n)$，则 $a \equiv b \bmod n$。

③ $a \equiv b \bmod n$,则 $b \equiv a \bmod n$。

④ $a \equiv b \bmod n$, $b \equiv c \bmod n$, 则 $a \equiv c \bmod n$。

✧ 从以上性质易知，同余类中的每一元素都可作为这个同余类的表示元素。

3.3 模运算

同余的性质

✧ 证明①：

若 $n|(a-b)$，则存在某个 k 使得$(a-b)=kn$。于是可知 $a=b+kn$。因此$(a \bmod n)=(b+kn$ 除以 n 的余数$)=(b$ 除以 n 的余数$)=(b \bmod n)$。

✧ 证明②：$a \equiv b \bmod n$,则 $b \equiv a \bmod n$

由 $a \equiv b \bmod n$，可得 $n|(a-b) \rightarrow n|(b-a)$，则 $b \equiv a \bmod n$。

✧ 证明③：$a \equiv b \bmod n$, $b \equiv c \bmod n$，则 $a \equiv c \bmod n$。

由 $a \equiv b \bmod n$, $b \equiv c \bmod n$,可得 $n|(a-b)$, $n|(b-c)$,则 $n|(a-b)+(b-c) \rightarrow n|(a-c)$。

3.3 模运算

模算术运算

- 求余数运算（简称求余运算）$a \bmod n$ 将整数 a 映射到集合$\{0,1,\ldots,n-1\}$，称求余运算在这个集合上的算术运算为模运算。
- 模运算有以下性质：

① $[(a \bmod n)+(b \bmod n)] \bmod n=(a+b) \bmod n$。

② $[(a \bmod n)-(b \bmod n)] \bmod n=(a-b) \bmod n$。

③ $[(a \bmod n)\times(b \bmod n)] \bmod n=(a\times b) \bmod n$。

3.3模运算

模算术运算

✧ 证明①：$[(a \bmod n)+(b \bmod n)] \bmod n=(a+b) \bmod n$

令$(a \bmod n)=r_a$, $(b \bmod n)=r_b$,于是存在整数 j, k 使得

$a= r_a +jn$，$b= r_b +kn$。那么

$$a+b \bmod n= (r_a +jn)+(r_b +kn) \bmod n$$

$$= (r_a + r_b+(k+j)n) \bmod n$$

$$= (r_a + r_b) \bmod n$$

$$=[(a \bmod n)+(b \bmod n)] \bmod n$$

3.3模运算

模算术运算

例： **11 mod 8=3; 15 mod 8=7**

[(11 mod 8)+(15 mod 8)]mod 8 =10 mod 8= 2

(11+15) mod 8= 26 mod 8= 2

[(11 mod 8)-(15 mod 8)]mod 8= -4 mod 8=4

(11-15) mod 8 = -4 mod 8=4

[(11 mod 8)×(15 mod 8)]mod 8 = 21 mod 8 = 5

(11×15) mod 8 = 165 mod 8 = 5

3.3模运算

模算术运算

幂运算和普通运算一样，可以通过反复乘法实现。

例：求 $11^7 \bmod 13$

$11^2=121\equiv 4 \pmod{13}$

$11^4=(11^2)^2=4^2\equiv 3 \pmod{13}$

$11^7=11\times 11^2\times 11^4$

$11^7=11\times 4\times 3=123\equiv 2 \pmod{13}$

3.3模运算

例：设 $Z_8=\{0,1,\ldots,7\}$，考虑 Z_8 上的模加法和模乘法。

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

×	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

- 加法：对每一 x，都有一 y，使得 $x+y\equiv 0 \bmod 8$。如对 2，有 6，使得 $2+6\equiv 0 \bmod 8$，称 y 为 x 的负数，也称为加法逆元。
- 乘法：对 x，若有 y，使得 $x\times y\equiv 1 \bmod 8$，如 $3\times 3\equiv 1 \bmod 8$，则称 y 为 x 的倒数，也称为乘法逆元。注意：并非每一 x 都有乘法逆元。

3.3模运算

一般地，定义 Z_n 为小于 n 的所有非负整数集合，即 $Z_n=\{0,1,\ldots,n-1\}$，称 Z_n 为模 n 的同余类集合。其上的模运算有以下性质：

① 交换律　$(w+x) \bmod n=(x+w) \bmod n$

$(w\times x) \bmod n=(x\times w) \bmod n$

② 结合律　$[(w+x)+y] \bmod n=[w+(x+y)] \bmod n$

$[(w\times x)\times y] \bmod n=[w\times(x\times y)] \bmod n$

③ 分配律　$[w\times(x+y)] \bmod n=[w\times x+w\times y] \bmod n$

④ 单位元　$(0+w) \bmod n=w \bmod n$

$(1\times w) \bmod n=w \bmod n$

⑤ 加法逆元　对 $w\in Z_n$，存在 $z\in Z_n$，使得 $w+z\equiv 0 \bmod n$，记 $z=-w$。

模运算的性质

此外还有以下性质：

- 如果$(a+b)\equiv(a+c) \bmod n$，则 $b\equiv c \bmod n$，称为加法的可约律。
  - 该性质可由上式两边同加上 a 的加法逆元得到。
  - 类似性质对乘法不一定成立。例如 $6\times3\equiv6\times7\equiv2 \bmod 8$，但 $3\neq7 \bmod 8$。
  - 原因：6 乘以 0 到 7 得到的 8 个数仅为 Z_8 的一部分。即如果将对 Z_8 作 6 的乘法 $6\times Z_8$（即用 6 乘 Z_8 中每一数）看作 Z_8 到 Z_8 的映射的话，Z_8 中至少有两个数映射到同一数，因此该映射为多到一的。
  - 所以对 6 来说，没有惟一的乘法逆元。但对 5 来说，$5\times5\equiv1 \bmod 8$，因此 5 有乘法逆元 5。仔细观察可见，与 8 互素的几个数 1，3，5，7 都有乘法逆元。
  - 这一结论可推广到任一 Z_n。

模运算的性质

- 定理：设 $a \in Z_n$，$\gcd(a, n)=1$，则 a 在 Z_n 中有乘法逆元。

证明：首先证明 a 与 Z_n 中任意两个不相同的数 b、c（不妨设 $c<b$）相乘，其结果必然不同。

否则设 $a \times b \equiv a \times c \mod n$，则存在两个整数 k_1, k_2，使得 $ab=k_1n+r$，$ac=k_2n+r$，可得 $a(b-c)=(k_1-k_2)n$，所以 a 是 $(k_1-k_2)n$ 的一个因子。又由 $\gcd(a, n)=1$，得 a 是 k_1-k_2 的一个因子，设 $k_1-k_2=k_3a$，所以 $a(b-c)=k_3an$，即 $b-c=k_3n$，与 $0<c<b<n$ 矛盾。

所以 $|a \times Z_n|=|Z_n|$。又知 $a \times Z_n \subseteq Z_n$，所以 $a \times Z_n=Z_n$。

因此对 $a \in Z_n$，存在 $x \in Z_n$，使得 $a \times x \equiv 1 \mod n$，即 x 是 a 的乘法逆元。记为 $x = a^{-1}$。（证毕）

3.3模运算

模运算的性质

- 设 p 为一素数，则 Z_p 中每一非 0 元素都与 p 互素，因此有乘法逆元。
- 类似于加法可约律，可有以下乘法可约律：

  如果$(a\times b)\equiv(a\times c) \bmod n$ 且 a 有乘法逆元，那么对$(a\times b)\equiv(a\times c) \bmod n$ 两边同乘以 a^{-1}，即得 $b\equiv c \bmod n$

求乘法逆元　　扩展欧几里得算法

海南大学 Hainan university

➢ 欧几里得算法

✓求两个正整数的最大公因子

✓推广的 **Euclid** 算法不仅可求两个正整数的最大公因子，而且当两个正整数互素时，还可求出其中一个数关于另一个数的乘法逆元。

求乘法逆元　扩展欧几里得算法

例 设a= 963和b= 657，① 求最大公因数 gcd(a,b)；

②求整数s,t，使得$as+bt$ = gcd(a,b)。

解：利用欧几里德算法可得

$963 = 1\times657+306$　　$9 = 7\times657 - 15\times(963 - 657) = 22\times657 - 15\times963$

$657 = 2\times306+45$　　$9 = 7\times(657 - 2\times306) - 306 = 7\times657 - 15\times306$

$306 = 6\times45 +36$　↓↑　$9 = 45 - (306 - 6\times45) = 7\times45 - 306$

$45 = 1\times36 + 9$　　$9 = 45 - 36$

$36 = 4\times9$

于是

① 963和657的最大公因数 gcd(963,657)= 9；

② s= −15, t= 22，使得

$$963 \times (-15) + 657 \times 22 = \gcd(963,657) = 9$$

✓ 求乘法逆元

- 如果gcd(a, b)=1，则b在mod a下有乘法逆元（不妨设$b<a$），即存在 x ($x<a$)，使得

$$b\,x \equiv 1 \mod a。$$

- 推广的Euclid算法先求出gcd(a, b)，当gcd(a, b)=1时，则返回b的逆元。

✓ 求乘法逆元

求　（1）$5^{-1} \bmod 97$

（2）$23^{-1} \bmod 67$

✓ 求乘法逆元

求　（1）$5^{-1} \bmod 97$

39

（2）$23^{-1} \bmod 67$

35

3.4 欧拉定理

3.4 欧拉定理

✓ **素数**

称整数 p (p>1)是素数，如果 p 的因子只有±1，±p

✓ **定理**

任一整数 a(a>1)都能惟一地分解为以下形式：

$$a = p_1^{a_1} p_2^{a_2} \cdots p_t^{a_t}$$

其中 p_1>p_2>…>p_t 是素数， $a_i > 0\ (i = 1, 2, \cdots t)$ **。例如**

91=7×13，11011=7×11²×13

3.4 欧拉定理

✧ **整数分解的唯一性：设 P 是所有素数集合，则任意整数 *a* (*a*>1)都能惟一地写成以下形式：**

$$a = \prod_{p \in P} p^{a_p}$$

其中 $a_p \geq 0$**，等号右边的乘积项取所有的素数，然而大多指数项** a_p **为 0。**

Fermat定理和Euler定理

Fermat 定理

- $a^{p-1} \equiv 1 \pmod{p}$
  - p是素数，gcd(a, p) = 1
- Fermat小定理
  - $a^p \equiv a \pmod{p}$
  - p是素数，a是任意整数
  - 在公钥密码中很有用

Euler函数 ø(n)

- 小于n且与n互素的正整数的个数

  如 n = 10,

  {0, 1, 2, 3, 4, 5, 6, 7, 8, 9} ， {1, 3, 7, 9}

  ø(10) = 4

- 素数 p　　ø(p) = p-1
- 素数p, q，有 ø(pq) = (p-1) x (q-1)
- 如:

  ø(37) = 36

  ø(21) = (3–1) x (7–1) = 2 x 6 = 12

- 约定： ø(1) = 1

- **定理：**

  设 $n = p_1^{e1} p_2^{e2} \cdots p_r^{er}$，$p_i \neq p_j$,$p_i$为素数，$e_i \geq 1$,

  则

  $$ø(n) = n\,(1-p_1^{-1})\,(1-p_2^{-1})\ldots(1-p_r^{-1})$$

- **例如：** $12 = 2^2 * 3$

  $$ø(12) = 12 * (1-2^{-1}) * (1-3^{-1}) = 4$$

Table 8.2 Some Values of Euler's Totient Function $\phi(n)$

n	$\phi(n)$	n	$\phi(n)$	n	$\phi(n)$
1	1	11	10	21	12
2	1	12	4	22	10
3	2	13	12	23	22
4	2	14	6	24	8
5	4	15	8	25	20
6	2	16	8	26	12
7	6	17	16	27	18
8	4	18	6	28	12
9	6	19	18	29	28
10	4	20	8	30	8

Euler 定理

- $a^{\phi(n)} \equiv 1 \pmod{n}$

  对任意 a, n，gcd(a,n) = 1

- 另一种表示：

  $a^{\phi(n)+1} \equiv a \pmod{n}$

  对任意 a, n

- 如：

  $a = 3; n = 10; \phi(10) = 4;$

  则 $3^4 = 81 \equiv 1 \bmod 10$

  $a = 2; n = 11; \phi(11) = 10;$

  则 $2^{10} = 1024 \equiv 1 \bmod 11$

Fermat定理是Euler定理的推论，或者说， Euler定理是Fermat定理的更一般化形式。

Euler 定理

- 与RSA有关的结果
  - 两个素数 p 和 q，整数m 和 n，n = pq, 0< m <n, 则有

$$m^{\phi(n)+1} = m^{(p-1)(q-1)+1} \equiv m \pmod{n}$$

  - 另一种表示：

$$m^{k\phi(n)+1} \equiv m \pmod{n}$$

3.5 中国剩余定理

3.5中国剩余定理

韩信点兵

韩信阅兵时，让一队士兵5人一行排队从他面前走过，他记下最后一行士兵的人数（1人）；再让这队士兵6人一行排队从他面前走过，他记下最后一行士兵的人数（5人）；再让这队士兵7人一行排队从他面前走过，他记下最后一行士兵的人数（4人），再让这队士兵11人一行排队从他面前走过，他记下最后一行士兵的人数（10人）。

然后韩信就凭这些数，可以求得这队士兵的总人数。

韩信点兵

韩信带贰仟伍佰士兵出去打仗，回营后，刘邦问士兵人数。韩信让士兵先列成五行纵队，末行一人；列成六行纵队，末行五人；列成七行纵队，末行四人；列成十一行纵队，末行十人。韩信立刻回答二千一百一十一人。刘邦惊为天人！

3.5中国剩余定理

1247年南宋的数学家秦九韶把《孙子算经》中“物不知其数”一题的方法推广到一般的情况，得到称之为“大衍求一术”的方法，在《数书九章》中发表。这个结论在欧洲要到十八世纪才由数学家高斯和欧拉发现。所以世界公认这个定理是中国人最早发现的，特别称之为“中国剩余定理”（Chinese remainder theorem）。

3.5中国剩余定理

孙子算经：

今有物不知其数，三三数之剩二，五五数之剩三，

七七数之剩二，问物几何？

3.5中国剩余定理

- **用于加速模运算**
- **某一范围内的整数可通过它对两两互素的整数取模所得的余数来重构**
- **使得非常大的数对M的模运算转化到更小的数上来进行运算**

3.5中国剩余定理

◆中国剩余定理

设 $(m_i, m_j)=1\ (1\le i<j\le n)$ ，$M=m_1m_2\cdots m_n$ ， 则同余组

$$x\equiv r_i \pmod{m_i} \qquad (i=1,2,\cdots,n)$$

的解为 $x\equiv\sum_{i=1}^{n}k_i\frac{M}{m_i}r_i \pmod{M}$。 其中$k_i$ 满足

$$k_i\frac{M}{m_i}\equiv 1 \pmod{m_i} \quad i=1,2,\cdots,n$$

3.5中国剩余定理

除数 m_i	余数 a_i	最小公倍数	衍数 $M_i = M/m_i$	乘率 M_i^{-1}	c_i	各总 $a_i c_i$	答数
m_1	a_1	$M=m_1m_2\ldots m_k$	M_1	M_1^{-1}			$A \equiv \left(\sum_{i=1}^{k} a_i c_i\right) (\mathrm{mod}\ M)$
m_2	a_2		M_2	M_2^{-1}			
…	…		…	…	…	…	
m_k	a_k		M_k	M_k^{-1}			

中国剩余定理

示例：$x \equiv 1(\mathrm{mod}19) \equiv 14(\mathrm{mod}17) \equiv 1(\mathrm{mod}12)$

$$x \equiv \sum_{i=1}^{n} k_i \frac{M}{m_i} r_i (\mathrm{mod}\ M)$$

$$M = 19 \times 17 \times 12 = 3876$$

$$M_1 = 17 \times 12 = 204 \quad M_2 = 19 \times 12 = 228 \quad M_3 = 19 \times 17 = 323$$

$$204k_1 \equiv 1(\mathrm{mod}19) \Rightarrow 14k_1 \equiv 1(\mathrm{mod}19) \Rightarrow k_1 = 15$$

$$228k_2 \equiv 1(\mathrm{mod}17) \Rightarrow 7k_2 \equiv 1(\mathrm{mod}17) \Rightarrow k_2 = 5$$

$$323k_3 \equiv 1(\mathrm{mod}12) \Rightarrow 11k_3 \equiv 1(\mathrm{mod}12) \Rightarrow k_3 = 11$$

$$\Rightarrow x \equiv 204 \times 15 \times 1 + 228 \times 5 \times 4 + 323 \times 11 \times 1 (\mathrm{mod}\ 3876)$$

$$\equiv 3193 (\mathrm{mod}\ 3876)$$

3.5中国剩余定理

应 用 举 例

- 孙子算经：
  - 今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何?
  - 答曰二十三

设所求物数为 X, 则

$$X \equiv 2 \pmod 3,$$

$$X \equiv 3 \pmod 5,$$

$$X \equiv 2 \pmod 7$$

3.5中国剩余定理

除数 m_i	余数 a_i	最小公倍数	衍数 $M_i = M/m_i$	乘率 M_i^{-1}	c_i	各总 $a_i c_i$	答数
3	2	M= 3*5*7 =105	5*7	2	5*7*2	70*2	140+63+30=233≡23 mod 105
5	3		7*3	1	7*3*1	21*3	
7	2		3*5	1	3*5*1	15*2	

3.6 离散对数

本原根

- $a^{ø(n)} \bmod n = 1$
- $a^m = 1 \pmod n$，$GCD(a, n) = 1$
  - 一定存在，因为$m = ø(n)$，（$ø(n)$是可能的最高指数）
  - m不一定最小
  - 一旦到达m, 将会产生循环。
  - 最小的m，成为a的阶。
- 如果一个数a的阶为$ø(n)$，则称a为n的本原根
- 若p是素数, a是p的本原根，则

  $a^1, a^2, a^3, \ldots, a^{p-1}$ 是模p各不相同的；
- 并不是所有整数模n都有本原根。
  - 只有n是形为2，4，p^α和$2\ p^\alpha$的整数才有本原根，其中p是奇素数，α是正整数。

本原根

计算

(1) $2^i \bmod 17$ $i=0,1,2,\ldots,16$

(2) $3^i \bmod 17$ $i=0,1,2,\ldots,16$

Table 8.3 Powers of Integers, Modulo 19

a	a^2	a^3	a^4	a^5	a^6	a^7	a^8	a^9	a^{10}	a^{11}	a^{12}	a^{13}	a^{14}	a^{15}	a^{16}	a^{17}	a^{18}
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
2	4	8	16	13	7	14	9	18	17	15	11	3	6	12	5	10	1
3	9	8	5	15	7	2	6	18	16	10	11	14	4	12	17	13	1
4	16	7	9	17	11	6	5	1	4	16	7	9	17	11	6	5	1
5	6	11	17	9	7	16	4	1	5	6	11	17	9	7	16	4	1
6	17	7	4	5	11	9	16	1	6	17	7	4	5	11	9	16	1
7	11	1	7	11	1	7	11	1	7	11	1	7	11	1	7	11	1
8	7	18	11	12	1	8	7	18	11	12	1	8	7	18	11	12	1
9	5	7	6	16	11	4	17	1	9	5	7	6	16	11	4	17	1
10	5	12	6	3	11	15	17	18	9	14	7	13	16	8	4	2	1
11	7	1	11	7	1	11	7	1	11	7	1	11	7	1	11	7	1
12	11	18	7	8	1	12	11	18	7	8	1	12	11	18	7	8	1
13	17	12	4	14	11	10	16	18	6	2	7	15	5	8	9	3	1
14	6	8	17	10	7	3	4	18	5	13	11	2	9	12	16	15	1
15	16	12	9	2	11	13	5	18	4	3	7	10	17	8	6	14	1
16	9	11	5	4	7	17	6	1	16	9	11	5	4	7	17	6	1
17	4	11	16	6	7	5	9	1	17	4	11	16	6	7	5	9	1
18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1	18	1

3.6离散对数

- 求 x，以满足 $y = g^x \pmod p$
- 可以写作 $x = \log_g y \pmod p$
- 如果g是p的本原根，则x一定存在；否则，不一定存在, 例如.

  $x = \log_3 4 \bmod 13$ 无解 （计算 $3^i \bmod 13$ （i=0,1，2,…,12））

  $x = \log_2 3 \bmod 13 = 4$

- 指数运算相对容易，求离散对数问题是困难的

3.6离散对数

- **定义：**

  若$m > 1, (a,m) = 1$, 则使得同余式 $a^i \equiv 1 (\mathrm{mod}\ m)$

  成立的最小正整数i，叫做a对模m的离散对数。

- **指数一定是欧拉函数的因子**
- **对任意整数b和模数p的本原根a，有唯一的幂i，使得**

  $b \equiv a^i \bmod p$, 其中$0 \le i \le p-1$

  该指数i称为以a为底模p的离散对数，记为 $\mathrm{dlog}_{a,\,p}(b)$

- **离散对数不仅与模有关，而且与本原根有关。**
- **例如：**
  - **2对模7的指数是3，对模11的指数是10，所以，2是模11的一个本原根，而不是模7的本原根；$\mathrm{dlog}_{2,\,9}(8) = 3$**

Table 8.4 Tables of Discrete Logarithms, Modulo 19

(a) Discrete logarithms to the base 2, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{2,19}(a)$	18	1	13	2	16	14	6	3	8	17	12	15	5	7	11	4	10	9

(b) Discrete logarithms to the base 3, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{3,19}(a)$	18	7	1	14	4	8	6	3	2	11	12	15	17	13	5	10	16	9

(c) Discrete logarithms to the base 10, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{10,19}(a)$	18	17	5	16	2	4	12	15	10	1	6	3	13	11	7	14	8	9

(d) Discrete logarithms to the base 13, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{13,19}(a)$	18	11	17	4	14	10	12	15	16	7	6	3	1	5	13	8	2	9

(e) Discrete logarithms to the base 14, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{14,19}(a)$	18	13	7	8	10	2	6	3	14	5	12	15	11	1	17	16	4	9

(f) Discrete logarithms to the base 15, modulo 19

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log_{15,19}(a)$	18	5	11	10	8	16	12	15	4	13	6	3	7	17	1	2	14	9


海南大学
Hainan university