§3.6　　整数和算法 (Integers and algorithms)

一．整数的表示

整数 965 可以表示成十进制数(以 10 为基(base)): $9\cdot10^2+6\cdot10+5$,也可以表示成以 2 为基的数(二进制数)，或以 8 为基的数(八进制数)等等。

一个整数 n 可以表示成以任意大于 1 的正整数 b 为基的数。

定理 1：设 b 是大于 1 的正整数。如果 n 是任一正整数，那么 n 可以唯一地表示成：

$$n=a_kb^k+a_{k-1}b^{k-1}+\cdots+a_1b+a_0$$

其中，k 是一非负整数，$a_0,a_1,\cdots,a_k$是小于 b 的非负整数且 $a_k\neq0$。

*定理 1 中的 n 的表示称为 n 的以 b 为基的展开式，记作 $(a_ka_{k-1}\cdots a_1a_0)_b$。

例如：$(245)_8=2\cdot8^2+4\cdot8+5.$

*以 2 为基的展开式称为二进制展开式(binary expansion)。

例 1：二进制展开式$(1\ 0101\ 1111)_2$的十进制数是什么？

解：$(1\ 0101\ 1111)_2=1\cdot2^8+0\cdot2^7+1\cdot2^6+0\cdot2^5+1\cdot2^4+1\cdot2^3+1\cdot2^2+1\cdot2^1+1\cdot2^0=351$。

例 3：将十进制数$(12345)_{10}$转化为八进制展开式(octal expansion).

解：12345$=8\cdot1543+1$

1543$=8\cdot192+7$

$192 = 8 \cdot 24 + 0$

$24 = 8 \cdot 3 + 0$

$3 = 8 \cdot 0 + 3$

于是: $(12345)_{10} = (30071)_8$。

*十六进制数的a_i取值 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A(10), B(11), C(12), D(13), E(14), F(15)。

例 4：求十进制数$(177130)_{10}$的十六进制展开式(hexadecimal expansion)。

解：$177130 = 16 \cdot 11070 + 10$

$11070 = 16 \cdot 691 + 14$

$691 = 16 \cdot 43 + 3$

$43 = 16 \cdot 2 + 11$

$2 = 16 \cdot 0 + 2$

于是：$(177130)_{10} = (2B3EA)_{16}$。

例 5：求十进制数$(241)_{10}$的二进制展开式。

解：$241 = 2 \cdot 120 + 1$

$120 = 2 \cdot 60 + 0$

$60 = 2 \cdot 30 + 0$

$30 = 2 \cdot 15 + 0$

$15 = 2 \cdot 7 + 1$

$7 = 2 \cdot 3 + 1$

$3 = 2 \cdot 1 + 1$

$1 = 2 \cdot 0 + 1$

于是：$(241)_{10} = (1111\ 0001)_2$。

算法 1：(10 进制转换为 b 进制展开式的算法)

PROCEDURE base b expansion (n: positive integer);

q:= n;

k := 0;

WHILE q$\neq 0$ DO

BEGIN

  $a_k := q \bmod b$;

  $q := \lfloor q/b \rfloor$;

  k := k+1;

END;

{the base b expansion of n is $(a_{k-1}a_{k-2} \cdots a_1 a_0)_b$}.

*二进制数转换为八进制、十六进制展开式。

例 6：$(11\ 1110\ 1011\ 1100)_2$转换为 16 进制展开式和 8 进制展开式。

解：(1) 转换为 16 进制展开式：从个位起，将 2 进制数每 4 位分为一个区段，得：0011, 1110, 1011, 1100, 再将每个区段转换为 16 进制数，得：3, E, B, C, 故

$(11\ 1110\ 1011\ 1100)_2 = (3EBC)_{16}$

(2) 转换为 8 进制展开式：从个位起，将 2 进制数每 3 位分为一个区段，得：011, 111, 010, 111, 100, 再将每个区段转换

为 8 进制数，得：3, 7, 2, 7, 4 故

$(11\ 1110\ 1011\ 1100)_2=(37274)_8$ 。

二．整数运算的算法

1. 加法：

例 7：求二进制数$(1110)_2$和$(1011)_2$的和。

解：从个位加起, $a=(a_3a_2a_1a_0)_2$, $b=(b_3b_2b_1b_0)_2$.

$a_0+b_0=0+1=0\cdot 2+1$, 有$c_0=0, s_0=1$

$a_1+b_1+c_0=1+1+0=1\cdot 2+0$, 有$c_1=1, s_1=0$

$a_2+b_2+c_1=1+0+1=1\cdot 2+0$, 有$c_2=1, s_2=0$

$a_3+b_3+c_2=1+1+1=1\cdot 2+1$, 有$c_3=1, s_3=1$

最后$s_4=c_3=1$, 得 $a+b=(s_4s_3s_2s_1s_0)_2=(11001)_2$。

*用竖式表示，见书 P251，图 1.

算法 2：（二进制加法）

PROCEDURE add (a, b: positive integers);

{the binary expansions of a and b are $(a_{n-1}a_{n-2}\cdots a_1a_0)_2$ and $(b_{n-1}b_{n-2}\cdots b_1b_0)_2$ }

c := 0;

FOR j := 0 TO $n-1$ DO

BEGIN

  d := $\lfloor (a_j+b_j+c)/2 \rfloor$;

  s_j := a_j+b_j+c-2d;

  c := d;

END;

s_n := c ;

{the binary expansion of the sum is $(s_n s_{n-1} \cdots s_0)_2$}.

2. 乘法：

设$a = a_k 2^k + a_{k-1} 2^{k-1} + \cdots + a_1 2 + a_0$

b= $b_{n-1} 2^{n-1} + b_{n-2} 2^{n-2} + \cdots + b_1 2 + b_0$

那么 ab= $a(b_0 2^0 + b_1 2^1 + \cdots + b_{n-1} 2^{n-1})$

$= a(b_0 2^0) + a(b_1 2^1) + \cdots + a(b_{n-1} 2^{n-1})$

例 9：求二进制数$a = (110)_2$和$b = (101)_2$的积。

解：$ab_0 \cdot 2^0 = (110)_2 \cdot 1 \cdot 2^0 = (110)_2$

$ab_1 \cdot 2^1 = (110)_2 \cdot 0 \cdot 2^1 = (0000)_2$

$ab_2 \cdot 2^2 = (110)_2 \cdot 1 \cdot 2^2 = (11000)_2$

然后求$(110)_2, (0000)_2, (11000)_2$三个数的和，得

$ab = (11110)_2$.

*写成竖式：见书 P252，图 2.

算法 3：（二进制乘法）

PROCEDURE multiply (a, b: positive integers);

{the binary expansions of a and b are $(a_{n-1} a_{n-2} \cdots a_1 a_0)_2$ and $(b_{n-1} b_{n-2} \cdots b_1 b_0)_2$,respectively}

FOR j := 0 TO $n - 1$ DO

BEGIN

IF $b_j = 1$ THEN $c_j :=$ a shifted j places

```
    ELSE  c_j := 0
END;
{c_0, c_1, ⋯ , c_{n−1}  are the partial products}
p := 0;
FOR  j := 0 TO n − 1 DO
    p := p + c_j  ;
{p is the value of ab }
```

3. 除法：

算法 4：（除和取模算法）

```
PROCEDURE division (a: integer; d: positive integer);
q := 0;
r :=  |a|;
WHILE  r  ≥ d  DO
BEGIN
    r := r − d;
    q := q + 1;
END;
IF  a < 0 and r > 0  THEN
BEGIN
    r := d − r;
    q :=  −(q + 1);
END;
```

{q = a div d is the quotient, r = a mod d is the remainder}.

三． 指数取模运算 (modular exponentiation)

*在密码学中，要求能有效地计算 $b^n \bmod m$，其中，b, n, m 都是大的整数。

设 $n = (a_{k-1}a_{k-2}\cdots a_0)_2$

$b^n = b^{a_{k-1}2^{k-1}+\cdots+a_1\cdot 2+a_0} = b^{a_{k-1}\cdot 2^{k-1}} b^{a_{k-2}\cdot 2^{k-2}} \cdots b^{a_1\cdot 2} b^{a_0}$

要计算b^n,我们先计算 b, $b^2, (b^2)^2 = b^4, (b^4)^2 = b^8, \cdots, b^{2^k}$, 然后把所有这样的项$b^{2^j}$乘起来，其中$a_j = 1$。

例如：要计算3^{11}，已知 11=$(1011)_2$.

因此，$3^{11} = 3^{1\cdot 2^3+0\cdot 2^2+1\cdot 2^1+1} = 3^8 \cdot 3^2 \cdot 3^1$，我们先算：3, $3^2 = 9, 3^4 = 9^2 = 81, 3^8 = 81^2 = 6561$，然后$3^{11} = 3^8 \cdot 3^2 \cdot 3^1 = 6561 \cdot 9 \cdot 3 = 177{,}147$.

因为是取模运算，我们算 b mod m, $b^2 \bmod m, b^4 \bmod m, \cdots, b^{2^{k-1}} \bmod m$，再对所有$a_j = 1$的项，将$b^{2^j} \bmod m$乘在一起，再取 mod m 运算。

算法 5：(指数取模运算)

PROCEDURE modular exponentiation (b : integer;

n= $(a_{k-1}a_{k-2}\cdots a_1a_0)_2$, m: positive integer);

x := 1;

power := b mod m;

FOR $i := 0$ TO $k-1$ DO

BEGIN

IF $a_i = 1$ THEN $x := (x \cdot \text{power}) \bmod m$;

$\text{power} := (\text{power} \cdot \text{power}) \bmod m$;

END;

{x equals $b^n \bmod m$}

四．欧几里德算法 (The Euclidean algorithm)

例子：求 gcd(91, 287).

解：首先，用小的那个数 91 去除大的数 287，得 $287 = 91 \cdot 3 + 14$, 因此，287 和 91 的任何公因子一定能整除$287 - 91 \cdot 3 = 14$. 故 gcd(91, 287) = gcd(14, 91). 再用 14 去除 91，得$91 = 14 \cdot 6 + 7$, 91 和 14 的任何公因子一定能整除$91 - 14 \cdot 6$=7。故 gcd(14, 91)=gcd(7, 14)。

再用 7 去除 14，得$14 = 7 \cdot 2$, 故 7 就是 7 和 14 的公因子，故 gcd(7, 14)=7, 从而 gcd(91, 287)=gcd(14, 91)=gcd(7, 14)=7。

引理 1：设 a=bq + r, 其中 a,b,q 和 r 都是整数，那么 gcd(a, b) = gcd(b, r)。

证明：如果我们能证明 a 和 b 的公因子就是 b 和 r 的公因子，那么就证明了 gcd(a, b)=gcd(b, r),因为这两对数有同样的最大公因子。

假设 d 整除 a 和 b，那么 d 也整除$a - bq = r$（由 3.4 节定理 1 得到）。因此，a 和 b 的任何公因子也是 b 和 r 的公因子。

类似地，假设 d 整除 b 和 r，那么 d 也整除 bq+r=a，因此，b 和 r 的任何公因子也是 a 和 b 的公因子。

结果有 gcd(a, b)=gcd(b, r)。

设 a, b 是正整数且$a \geq b$，令$r_0 = a$，$r_1 = b$，反复应用除算法，我们得到:

$$r_0 = r_1 q_1 + r_2 \qquad 0 < r_2 < r_1$$

$$r_1 = r_2 q_2 + r_3 \qquad 0 < r_3 < r_2$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_{n-1} + r_n \qquad 0 < r_n < r_{n-1}$$

$$r_{n-1} = r_n q_n$$

因为$a = r_0 > r_1 > r_2 > \cdots \geq 0$, 该算法必然终止。反复应用引理 1，有 $\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{n-2}, r_{n-1}) = \gcd(r_{n-1}, r_n) = r_n$.

算法 6：（欧几里德算法）

```
PROCEDURE gcd (a, b: positive integers);
x := a;
y := b;
WHILE  y ≠ 0  DO
BEGIN
   r := x mod y;
   x := y;
   y := r;
END;
{gcd(a, b) is x}
```

§3.7　数论的应用

一．　一些有用的结果

定理 1：设 a 和 b 是正整数，那么存在整数 s 和 t 使得 gcd(a,b)=sa+tb。

*我们不给出正式的证明，但通过用欧几里德算法求最大公因子的例子说明。

例 1：将 gcd(252, 198)=18 表示成 252 和 198 的线性组合(linear combination).

解：用欧几里德算法求 gcd(252, 198)=18 的过程如下：

$$252 = 1\cdot 198 + 54 \qquad (1)$$

$$198 = 3\cdot 54 + 36 \qquad (2)$$

$$54 = 1\cdot 36 + 18 \qquad (3)$$

$$36 = 2\cdot 18 \qquad (4)$$

由(3)式，有$18 = 54 - 1\cdot 36$，由(2)式 $36 = 198 - 3\cdot 54$.
代入上式，得

$$18 = 54 - 1\cdot(198 - 3\cdot 54) = 4\cdot 54 - 1\cdot 198 \qquad (5)$$

再由(1)式，有$54 = 252 - 1\cdot 198$，代入(5)式，得

$$18 = 4\cdot(252 - 1\cdot 198) - 1\cdot 198 = 4\cdot 252 - 5\cdot 198$$

这就是我们要求的解。

引理 1：如果 a,b,c 是正整数并且 gcd(a,b)=1 和$a|bc$,那么 $a|c$。

证明：因为 gcd(a, b)=1，由定理 1，存在整数 s 和 t，有

$$sa + tb = 1$$

上式两边同时乘以 c，有 $sac + tbc = c.$

由 3.4 节定理 1，由该定理中(ii)，有$a|tbc$，又因为$a|sac$和$a|tbc$，由该定理(i)，有$a|(sac + tbc)$，即$a|c$。

引理 2：如果 p 是素数且$p|a_1 a_2 \cdots a_n$，其中每个a_i是整数，那么$p|a_i$对某个 i 成立。

*我们现在证明整数的素数因子分解是唯一的，即 3.5 节定理 1 中表示的唯一性。

证明：用反证法。假设正整数 n 可以表示成两组不同的素数的乘积，即$n = p_1 p_2 \cdots p_s$且$n = q_1 q_2 \cdots q_t$，其中每个p_i和q_j都是素数，并且$p_1 \le p_2 \le \cdots \le p_s$和$q_1 \le q_2 \le \cdots \le q_t$。

由于$n = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t$，我们删除两组素数中共同的素数（公因子），有$p_{i_1} p_{i_2} \cdots p_{i_u} = q_{j_1} q_{j_2} \cdots q_{j_v}$。

这时，等式两边没有共同的素数且 u 和 v 是正整数。由引理 1，左边的p_{i_1}整除q_{j_k}对某个 k 成立，但任何一个素数不能整除另一个素数，得到矛盾。从而 n 的非递减的素数因子分解是唯一的。

*同余关系对乘法保持同余，但对除法不一定。

例 2：已知$14 \equiv 8 \pmod 6$，但两边同时除以 2，左边是$\frac{14}{2} = 7$，右边是$\frac{8}{2} = 4$，但$7 \not\equiv 4 \pmod 6$。

定理 2：设 m 是正整数，并设 a,b,c 是整数，如果

$ac \equiv bc \pmod{m}$且 gcd(c, m)=1，那么$a \equiv b \pmod{m}$。

证明：因为$ac \equiv bc \pmod{m}$，$m|(ac-bc) = c(a-b)$．由引理 1，因为 gcd(c, m)=1，因此$m|(a-b)$，从而有 $a \equiv b \pmod{m}$.

二． 线性同余式

同余式$ax \equiv b \pmod{m}$，其中 m 是正整数，a 和 b 是整数，x 是变量，称为线性同余式(linear congruence).

如果存在整数$\bar{a}$使得$\bar{a}a \equiv 1 \pmod{m}$，那么$\bar{a}$称为 a 模 m 的逆元(inverse of a modulo m)。

定理 3：如果 a 和 m 是互素的整数且$m > 1$。那么 a 模 m 的逆元存在．进一步，这个逆元在模 m 意义下是唯一的。（即存在唯一的正整数$\bar{a} < m$，且$\bar{a}a \equiv 1 \pmod{m}$且任何 a 模 m 的逆元都与$\bar{a}$模 m 同余）。

证明：由定理 1，因为 gcd(a, m)=1，存在整数 s 和 t，使得

$$sa + tm = 1$$

这意味着$sa + tm \equiv 1 \pmod{m}$。但$tm \equiv 0 \pmod{m}$，所以

$$sa \equiv 1 \pmod{m}$$

结果，s 是 a 模 m 的逆元，这个逆元模 m 是唯一的。证明如下：

假设还存在另一个逆元 r，有 $ra \equiv 1 \pmod{m}$

由 3.4 节的练习，有$(sa - ra) \equiv (1-1) = 0 \pmod{m}$，即$m|(sa-ra) = a(s-r)$。又因为 gcd(a, m)=1，由引理 1，$m|(s-r)$，故 s 和 r 模 m 同余。

例 3：求 3 模 7 的逆元。

解：因为 gcd(3，7)=1，由定理 3 知，3 模 7 的逆元存在。由欧几里德算法，$7=2\cdot 3+1$，从而有$(-2)\cdot 3+1\cdot 7=1$，故-2是 3 模 7 的逆元。与-2同余的数还有 5，$-9, 12$等都是 3 模 7 的逆元。

例 4：（求解模线性方程）以下模线性方程的解是什么？

$$3x\equiv 4\ (\mathrm{mod}\ 7)$$

解：由例 3 知，-2是 3 模 7 的逆元，线性方程两边乘-2，得 $(-2)\cdot 3x\equiv(-2)\cdot 4(\mathrm{mod}\ 7)$.

因为$-6\equiv 1\ (\mathrm{mod}\ 7)$和$-8\equiv 6(\mathrm{mod}\ 7)$，所以，x 的解是

$$x\equiv -8\equiv 6\ (\mathrm{mod}\ 7).$$

我们要确定满足$x\equiv 6\ (\mathrm{mod}\ 7)$的每个 x 都是一个解。设$x\equiv 6(\mathrm{mod}\ 7)$，由 3.4 节定理 5，有

$$3x\equiv 3\cdot 6=18\equiv 4(\mathrm{mod}\ 7)$$

故所有满足$x\equiv 6(\mathrm{mod}\ 7)$的 x 都是方程的解。

三．中国剩余定理(The Chinese Remainder Theorem)

定理 4：（中国剩余定理）设$m_1, m_2, \cdots, m_n$是两两互素的正整数且$a_1, a_2, \cdots, a_n$是任意整数，那么同余方程组

$$\begin{aligned} x &\equiv a_1\ (\mathrm{mod}\ m_1)\\ x &\equiv a_2\ (\mathrm{mod}\ m_2)\\ &\vdots\\ x &\equiv a_n\ (\mathrm{mod}\ m_n)\end{aligned}$$

有模$m = m_1 m_2 \cdots m_n$唯一的解(即存在解 x 满足$0 \le x < m$并且任何其它解都模 m 与 x 同余)。

证明：我们将证明解存在并且唯一。为了构造联立方程组的解，首先设　$M_k = \frac{m}{m_k}$，$k = 1,2,\cdots,n.$

因为m_i和m_k互素（当$i \neq k$时），$\gcd(m_k, M_k) = 1$，由定理 3，我们知道存在y_k是M_k模m_k的逆元,满足：$M_k y_k \equiv 1 (\mathrm{mod}\ m_k)$。

我们现在构造方程组的联立解：

$$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$$

我们将证明 x 是联立解。首先注意到$M_j \equiv 0\ (\mathrm{mod}\ m_k)$对$j \neq k$成立，x 中所有项除了第 k 项外，模$m_k$余数为 0.又因为$M_k y_k \equiv 1\ (\mathrm{mod}\ m_k)$，有

$$x \equiv a_k M_k y_k \equiv a_k\ (\mathrm{mod}\ m_k),\ \ k = 1,2,\cdots,n$$

因此，x 是上述联立方程的解。该解的唯一性证明留作练习。

例 6：设有$x \equiv 2\ (\mathrm{mod}\ 3), x \equiv 3\ (\mathrm{mod}\ 5), x \equiv 2\ (\mathrm{mod}\ 7)$，求解 x.

解：设$m = 3 \cdot 5 \cdot 7 = 105, M_1 = \frac{m}{3} = 35, M_2 = \frac{m}{5} = 21,$ $M_3 = \frac{m}{7} = 15$. 我们得到 2 是$M_1 = 35$模 3 的逆元，因为$35 \equiv 2 (\mathrm{mod}\ 3)$， 1 是$M_2 = 21$模 5 的逆元，因为$21 \equiv 1 (\mathrm{mod}\ 5)$，1 是$M_3 = 15$模 7 的逆元，因为$15 \equiv 1 (\mathrm{mod}\ 7)$。因此联立解 x 为:

$$\begin{aligned} x &= a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 \\ &= 2 \cdot 35 \cdot 2 + 3 \cdot 21 \cdot 1 + 2 \cdot 15 \cdot 1 \end{aligned}$$

$= 233 \equiv 23 (\mathrm{mod}\ 105)$

因此，23 是最小的正整数联立解。

四． 费马小定理

定理 5：如果 p 是素数且 a 是一个不能被 p 整除的整数，那么 $a^{p-1} \equiv 1\ (\mathrm{mod}\ p)$,

进一步，对每一个整数 a，我们有

$a^{p} \equiv a\ (\mathrm{mod}\ p)$。

作业：

1. 将以下十进制数转换为二进制数，再转换为八进制数和十六进制数。

（1） 231 ； （2） 321 。

2. 用欧几里德算法求以下最大公因子：gcd(1000, 5040).

3. 用中国剩余定理求以下联立同余方程的解：

$x \equiv 2\ (\mathrm{mod}\ 3); x \equiv 1\ (\mathrm{mod}\ 4); x \equiv 3\ (\mathrm{mod}\ 5).$

4. 求解模线性方程：$7x \equiv 5\ (\mathrm{mod}\ 11)$.