§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)):

,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：

其中，k是一非负整数，是小于b的非负整数且。

\*定理1中的n的表示称为n的以b为基的展开式，记作

。

例如：.

\*以2为基的展开式称为二进制展开式(binary expansion)。

例1：二进制展开式的十进制数是什么？

解：。

例3：将十进制数转化为八进制展开式(octal expansion).

解：12345

1543

192

24

3

于是: 。

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

例4：求十进制数的十六进制展开式(hexadecimal expansion)。

解：

11070

691

43

2

于是：。

例5：求十进制数的二进制展开式。

解：241

120

60

30

15

7

3

1

于是：。

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 DO

BEGIN

;

k := k+1;

END;

{the base b expansion of n is }.

\*二进制数转换为八进制、十六进制展开式。

例6：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

(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

。

二．整数运算的算法

1. 加法：

例7：求二进制数和的和。

解：从个位加起, , .

最后, 。

\*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 and

}

c := 0;

FOR j := 0 TO DO

BEGIN

;

c := d;

END;

c ;

{the binary expansion of the sum is }.

2. 乘法：

设

b

那么ab

例9：求二进制数和的积。

解：

然后求三个数的和，得

.

\*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 and

,respectively}

FOR j := 0 TO DO

BEGIN

IF THEN

ELSE

END;

{ are the partial products}

p := 0;

FOR

;

{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 := ;

WHILE DO

BEGIN

;

END;

IF THEN

BEGIN

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 , 其中，b, n, m都是大的整数。

设

要计算,我们先计算b, , 然后把所有这样的项乘起来，其中。

例如：要计算，已知11=.

因此，，我们先算：3, 然后

因为是取模运算，我们算 b mod m,

, 再对所有的项，将乘在一起，再取mod m运算。

算法5：(指数取模运算)

PROCEDURE modular exponentiation (b : integer;

n, m: positive integer);

x := 1;

power := b mod m;

FOR

BEGIN

IF

END;

{x equals

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, 因此，287和91的任何公因子一定能整除 故gcd(91, 287) = gcd(14, 91). 再用14去除91，得 91和14的任何公因子一定能整除=7。故gcd(14, 91)=gcd(7, 14)。

再用7去除14，得, 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（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，令，，反复应用除算法，我们得到:

因为 该算法必然终止。反复应用引理1，有.

算法6：（欧几里德算法）

PROCEDURE gcd (a, b: positive integers);

x := a;

y := b;

WHILE DO

BEGIN

r := x mod y;

x := y;

y := r;

END;

{gcd(a, b) is x}

§3.7 数论的应用

1. 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：

3）

4）

由(3)式，有

代入上式，得

(5)

再由(1)式，有，代入(5)式，得

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和那么a。

证明：因为gcd(a, b)=1, 由定理1，存在整数s和t, 有

上式两边同时乘以c，有

由3.4节定理1, 由该定理中(ii), 有, 又因为和

由该定理(i)，有 即。

引理2：如果p是素数且其中每个是整数，那么对某个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，即且，其中每个和都是素数，并且和。

由于，我们删除两组素数中共同的素数（公因子），有

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，左边的整除对某个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：已知但两边同时除以2，左边是右边是但。

定理2：设m是正整数，并设a,b,c是整数，如果且gcd(c, m)=1，那么。

证明：因为, 由引理1，因为gcd(c, m)=1，因此

1. 线性同余式

同余式其中m是正整数，a和b是整数，x是变量，称为线性同余式(linear congruence).

如果存在整数使得，那么称为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。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，且且任何a模m的逆元都与模m同余）。

证明：由定理1，因为gcd(a, m)=1, 存在整数s和t，使得

这意味着。但，所以

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

由3.4节的练习, 有，即

。又因为gcd(a, m)=1，由引理1，

，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，，从而有，故是3模7的逆元。与同余的数还有5, 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？

解：由例3知，是3模7的逆元，线性方程两边乘，得 .

因为和，所以，x的解是

.

我们要确定满足的每个x都是一个解。设

, 由3.4节定理5，有

故所有满足的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）设是两两互素的正整数且是任意整数，那么同余方程组

有模唯一的解(即存在解x满足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

因为和互素（当），，由定理3，我们知道存在是模的逆元,满足：。

我们现在构造方程组的联立解：

我们将证明x是联立解。首先注意到对成立，x中所有项除了第k项外，模余数为0.又因为，有

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，求解x.

解：设

. 我们得到2是模3的逆元，因为，1是模5的逆元，因为，1是模7的逆元，因为。因此联立解x为:

因此，23是最小的正整数联立解。

1. 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 ,

进一步，对每一个整数a，我们有

。

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。
2. 231 ； （2） 321 。
3. 用欧几里德算法求以下最大公因子：gcd(1000, 5040).
4. 用中国剩余定理求以下联立同余方程的解：

.

1. 求解模线性方程：