文章编号:1005－0523(2007)02－0100－03

大整数运算的基选择

刘觉夫,周　娟

(华东交通大学 信息工程学院 江西 南昌 330013)

摘要:在较多的编程语言中,整数的最大值小于 2^{63}.一旦计算超出了这个范围.值就不再是正确的了.研究了大整数基的选择,提出合理选择基的方法.还给出 1 个用到大整数但不需要用到大整数的运算方法.

关　键　词:大整数;算法;编程竞赛

中图分类号:TP301.6　　　　**文献标识码**:A

在较多的编程语言中,整数一般有 3 种:短整数($-2^{15}-2^{15}-1$),整数($-2^{31}-2^{31}-1$),长整数($-2^{63}-2^{63}-1$).最大整数是 19 位数 $2^{63}-1=9223372036854775807$.在 C 或 C++中(下同)这 3 种数据类型为:short int,int,__int64;__int64 型的输入输出格式为“%I64d”.一旦计算超出了这个范围.值就不在是正确的了.把超过 2^{63}的数称为大整数.在许多研究中,比如计算机代数学(Comput Algebra),几何论证(Geometric Reasoning),密码学,微观模拟(如生物信息,基因工程,数量遗传)等,需要大整数的运算,要用到几百位上千位甚至上万位的整数运算.计算机科学家就开发不少这一类具有无限精确度的软件,例如 MACSYMA,MATHEMATICA 等都是有名的例子.在最近几年兴盛起来的计算机程序设计竞赛中,都少不了大整数的运算,在这些运算中大整数一般在几千位整数的范围内,他们用的大多数是 C,C++,Pascal 等语言,每所大学,甚至有不少中学都有相当一部分人为竞赛而使用大整数运算.在各种编程语言中,解决的办法是用数组表示整数,例如 a=12345,这个数用数组表示为:a[1]=1,a[2]=2,a[3]=3,a[4]=4,a[5]=5;a[0]=5 表示 a 是 5 位数,实际上这个数是 $a=a[1]*10^4+a[2]*10^3+a[3]*10^2+a[4]*10+a[5]$;这时称 a 用 10 进制数表示.a 也可以用 a[1]=1;a[2]=23,a[3]=45,a[0]=3 表示,实际上这个数是 $a=a[1]*10^4+a[2]*10^2+a[3]$;这时称 a 用 10^2 进制数表示.如果数组 a 是__int64 型整数,那么 1 个整数可用 10 进制,10^2 进制,10^3 进制,一直到 10^9 进制表示.这就是用多个整数表示 1 个整数.使用 10^w 进制,1 个 m 位整数就用 m/w 个整数表示.一个整数用 base 进制表示,就称它的基是 base.base 为多大为好呢?

设 a 是 m 位数,b 是 n 位整数.以乘法运算为例.如果用 10 进制,要进行 mn 次乘法运算,如果用 10^9 进制,要进行 mn/81 次乘法运算.这样看来,进制越大,运算次数越少,速度越快.如果用 10^{10}进制,则 2 数相乘,乘积超过 2^{63}.所以基最大为 10^9.如果数组定义为 int 型,基最大为 10^4.数组定义为 char 型,基最大为 10^5.实际上,如果数组定义为 unsigned char 型,基可以定义为 10^2.char 型为 1 个字节,__int64 型为 8 个字节.如果使用__int64 型,基用 10^9,则 8 个字节表示整数的 9 个数字,每个字节表示 9/8 个数字,如果使用 unsigned char 型,基用 10^2,则 1 个字节表示整数的 2 个数字,每个字节表示 2 个数字,这是占用空间最少的,而算次数最少的.本文经过大量的计算实验,提出如何合理地选择基,本文还给出某些涉及到大整数但不用大整数就可以得到正确结果的方法.

1) 大整数乘法基的选择.设 a 是 m 位数,b 是 n

收稿日期:2007－03－27

作者简介:刘觉夫(1963－),男,湖南平江人,教授.

位数，则乘积 ab 是 m＋n 位数或 m＋n－1 位数．令 m＝n＝20000，用随机函数产生了两个 20000 位的整数 a，b．a 的最大的 10 位数是 a＝9149825115 b 的最大的 10 位数是 b＝9704845712，

基选择 char 型 10 进制，unsigned char 型 10^2 进制运行的结果如下

char 型 10 进制 开始时间 2061，结束时间 2073，运行时间 12 秒

unsigned char 型 10^2 进制 开始时间 2073，结束时间 2077，运行时间 4 秒

基选择 int 型 10^2 进制，10^3 进制，10^4 进制运行的结果如下

10^2 进制 开始时间 2077，结束时间 2085，运行时间 7 秒

10^3 进制 开始时间 2085，结束时间 2088，运行时间 3 秒

10^4 进制 开始时间 2088，结束时间 2090，运行时间 2 秒

基选择_ int64 型运行的结果如下

10^4 进制 开始时间 2090，结束时间 2093，运行时间 3 秒

10^5 进制 开始时间 2093，结束时间 2096，运行时间 3 秒

10^6 进制 开始时间 2096，结束时间 2097，运行时间 1 秒

10^7 进制 开始时间 2097，结束时间 2098，运行时间 1 秒

10^8 进制 开始时间 2098，结束时间 2099，运行时间 1 秒

10^9 进制 开始时间 2099，结束时间 2100，运行时间 1 秒

令 m＝n＝10000，运行的结果如下

unsigned char 型 10^2 进制，运行时间 1 秒

int 型 10^2 进制，运行时间 2 秒

int 型 10^3 进制，运行时间 1 秒

由上述计算可知基越大运行速度越快．提出如下选择基的方法．

选择基的方法：当 a，b 的位数之积 m＊n＜＝10^8 时，使用 unsigned char 型 10^2 进制，只用到加法，运算速度快，占用空间小（每个字节存 2 个整数位），m＊n＞10^8 时，使用_ int64 型 10^9 进制，运算速度快，占用空间小（每个字节存 9/8 个整数位）．

上述运算的代码如下：（unsigned char 型 10^2 进制，只要稍微修改，就得到其他进制的代码）

```
M=m/2;N=n/2;
 k=M+N-1;base=100;

 for(i=0;i<=k;i++)z[i]=0;
 for(i=1,s=0;i<=M;i++,s++)
 {
  for(j=1,t=0;j<=N;j++,t++)
  { //z[s+j]+=x[i]*y[j];
   z[s+j]+=L[x[i]][y[j]];
   //L[e][f]  =e*f%100;
   z[s+t]+=H[x[i]][y[j]];
   //H[e][f] =e*f/100;
   }
   for(j=k;j>=1;j--)
   {
    if(z[j]>=base){
    z[j-1]+=div100[z[j]];z[j]=mod100[z[j]];
    //div100[e]=e/100; mod100[e]=e%100;
    }
   }
  }
if(z[0]>0){printf("%u",z[0]);printf("%02u",z[1]);}
else printf("%u",z[1]);
for(i=2;i<=k;i++)pr("%02u",z[i]);
pr("\n");
```

如果 a＊b 的值不超过整数类型最大值的平方，a＞b，b 是 n（＜＝9）位数，则算法可简化．将 a 用 $10^{(18-n)}$ 进制数表示．例如 a＝123451234567890，b＝7654321．a 是 15 位数，b 是 7 位数，a＊b 是 21 或 22 位的大整数．a＝a1＊10^{11}＋a2；a1＝1234，a2＝51234567890．算法代码为：

```
M=100000000000;
a1=a1*b;
a2=a2*b;
if(a2>=M)
{
 a1+=a2/M;
  a2%=M;
}
```

//输出运算结果

printf("%I64d%011I64d\n",a1,a2);

//("%011I64d",a2) 输出64位整数a2,如果a2不满11位则左边补零.

显然,这比用数组简单明了.目前在国际国内的计算机程序设计竞赛中有大量的计算题可用这个简化算法[3][4].

2) 参与运算的数和运算结果在整数范围内,但中间结果超出整数范围.

例 计算组合数C(m,n),它表示从m个元素中取n个的取法数.C(m,n)=m! /n! /(m-n)!.这种计算即使m很小也会超出整数范围.一般的算法是C(m,n)=m*(m-1)/2*(m-2)/3*…*(m-n+1)/n.即乘1数除1数再乘1数除1数这样的算法.归结为d=a*b/c的运算类型,a*b超出整数范围,但a*b/c在整数范围内.算法如下:设该种整数类型的最大值为M

2.1)c<M的平方根

k=a/c;

r=a%c;//a=k*c+r r<c a*b/c=k*b+r*b/c

//a*b/在整数范围内,所以k*b也在整数范围内

d=k*b;

l=b/c;

s=b%c;//b=l*c+s s<c r*b/c=r(l*c+s)/c=r*l+r*s/c

d=d+r*l+r*s/c

//r<c,s<c,r*c不超过最大整数.

由于运算的结果在整数范围内,因此r*l,r*s也在整数范围内

2.2)c>=M的平方根.文献[2]给出的计算d=a*b/c的方法如下:

k=gcd(a,c);

//k是a,c的最大公因数

a=a/k;

c=c/k;

b=b/c;

d=a*b;

3)大整数除整数c=a/b,r=a%b.b是位数小于等于17的整数.数组表示a

设a为m位数,b为n位数,则c=a/b为k=m-n+1或k-1位数,将a用数组表示:a[1]a[2]…a[m].算法如下.

```
r=0;
for(j=1;j<=n;j++)r=r*10+a[j];
for(j=1,s=n;j<=k;j++,s++)
{
  c[j]=r/b;
  r=r%b; if(j<k)r=r*10+a[s+1];

}
```

// r=a%b是余数,如果c[1]>0则c是m-n+1位数,

```
if(c[1]>0)printf("%d",c[1]);
for(j=2;j<=k;j++) printf("%d",c[j]);
printf("     %d\n",r);
```

参考文献:

[1]冼镜光.C语言名题精选百则技巧篇[M].北京:机械工业出版社,2005.

[2]周尚超.整数运算中的问题和解决办法[J].华东交通大学学报,2005,(2):155-157.

[3]http://acm.pku.edu.cn/JudgeOnline/

[4]http://acm.hdu.edu.cn

[5]李文化,董克家.大整数精确运算的数据结构与基选择[J].计算机工程与运用.2006,(32):24-26.

Radix's Selection of Big Integral's calculating Accurately

LIU Jue-fu,ZHOU Juan

(School of Information Eng.,East China Jiaotong University,Nanchang 330013,China)

Abstract:Of most programming languages,the maximum value of the integer should be small than 2^{63},the value will not be correct once the calculation goes beyond the range.The problem of integer operation can be solved if several integers can be integral into one.

Key words:big integer;algorithm;programming contest