计算机程序语言在初等数论中的应用

多布杰
(西藏大学理学院 西藏拉萨 850000)

摘要：随着电子计算机的诞生和信息时代的到来，计算机与数论的关系越来越密切。这不仅体现在计算机在数论中的广泛应用，还体现在数论在计算机技术和网络领域的重大作用。尤其是计算机高级程序语言的诞生对数论的研究提供了强有力的工具。文章主要介绍计算机程序语言在的标准分解、Euler 函数、中国剩余定理、Legendre 符号等初等数论问题中的应用。

关键字：C 语言；初等数论；应用；Euler 函数；中国剩余定理
中图分类号：TP312　文献标识码：A　文章编号：1005-5738(2009)01-113-04

数论这门学科最初是从研究整数开始的，所以叫做整数论。后来整数论又进一步发展，就叫做数论了。确切的说，数论就是一门研究整数性质的学科。它是数学中最抽象、最古老、最“纯粹”的一个重要分支。数论作为一门独立的学科，按照研究方法来说，可以分成初等数论、解析数论、代数数论和几何数论四个部分。而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。但随着数学其他分支的发展，研究初等数论的方法也在不断拓展。尤其是随着计算机技术的发展和信息时代的到来，计算机与初等数论的联系也十分密切。一方面计算机技术在初等数论中有着广泛的应用，如构造容量更大的质数表、发现更大的梅森(Mersenne)质数、大数的分解、Legendre 符号的计算等问题的研究中都要用到计算机技术。另一方面，数论在计算机科学中也有重要作用，如寻找梅森素数是测试计算机运算速度及其它功能的有力手段。如第 34 个梅森质数(目前只发现了 46 个梅森质数)就是 1996 年 9 月美国克雷公司在测试其最新超级计算机的运算速度时得到的。同时发现梅森质数也促进了算法与程序设计技术的发展等。

当然，本文只是通过证实初等数论中的几个重要结论，介绍计算机程序语言在初等数论中的应用。

1　求最大公因数

整除理论是初等数论的基础，而最大公因数理论是整除理论的核心内容。其中求自然数的最大公因数是一个很实际的问题。辗转相除法是求最大公因数的最简单且最有效的方法。

问题：求(1859，1573)。

```
#include "Stdio.h"
#include "Conio.h"
 long int main(void)
{
 long int n=0,m=0,temp=0,r;
 scanf("%ld%ld",&m,&n);
 if(m<n){
 temp=m;
 m=n;
n=temp;
}
```

收稿日期：2008-12-17
作者简介：多布杰(1972-)，男，藏族，西藏日喀则人，西藏大学理学院副教授，主要研究方向为初等数论。

© 1994-2012 China Academic Journal Electronic Publishing House. All rights reserved.　http://www.cnki.net

```
r=m%n;
while(r!=0){
 m=n;
 n=r;
 r=m%n;
 }
printf("The MAX is %ld\n",n);
 }
```

运行结果为：

1859 1573

The MAX is 143

2 $n!$的标准分解式

算术基本定理是初等数论中最重要、最基本、最著名的定理之一。它的内容是：任一大于 1 的整数必能唯一地表成质数的乘积[1]。一个整数的标准分解式给很多问题带来方便。然而，我们知道把一个整数分解成标准分解式是没有一般方法的。但对于特殊的整数 $n!$，我们利用函数$[x]$的性质可以求出 $n!$的标准分解式。显然，对于这个问题关键是算出小于 n 的质数在 $n!$内的最高次幂。这里就结合一个具体的实例来给出如何算出这个最高次幂的程序。

问题 求 7 在 2006!内的最高次幂。

程序为：

```
#include "Stdio.h"
#include "Conio.h"
int main(void)
{
long int p,n,a=0,t;
printf("Input number:");
scanf("%ld",&n);
printf("Input prime number:");
scanf("%ld",&p);
t=n/p;
a=a+t;
while(t!=0)
{
n=t;
t=n/p;
a=a+t;
}
printf("a=%ld\n",a);
}
```

运行结果：

Input number:2006

Input prime number:7

a=331

3 *Euler* 函数的计算

所谓 $Euler$ 函数 $\varphi(n)$是表示序列 0,1,2,···,n-1 中与 n 互质的正整数的个数[2]。若知道了 n 的所有质因数，$\varphi(n)$的计算并不困难。因为我们有公式 $\varphi(n)=n\prod_{i=1}^{k}(1-\frac{1}{p_i})$，其中 $p_i(i=1,2,\cdots k,)$为 n 的不同质因数[3]。由于求出 n 的因数比较困难，下面的程序中并没有利用上述公式，而是根据定义用一个循环语句和辗转相除法检验从 1 到 n 的自然数中哪些与 n 互质，并同时以计数的方法来算出 $\varphi(n)$。

```
#include "Stdio.h"
#include "Conio.h"
int main()
{
long int n,m,t=0,a,b,q,r,temp;
printf("Input number:");
scanf("%ld",&n);
for(m=1;m<n;m++)
{a=n,b=m;
if(a<b)
{temp=a;
 a=b;
 b=temp;
 }
 r=a%b;
 while(r!=0)
 {a=b;
 b=r;
 r=a%b;
 }
 if(b==1)
 t=t+1;
 }
 printf("Euler=%ld\n",t);
 }
```


© 1994-2012 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

运行结果：

```
Input number:25296
Euler=7680
```

4 中国剩余定理 (孙子定理)

在国外文献中被称为“中国剩余定理”的是我国古代的《孙子算经》里提出的解决一次同余式组的方法加以推广后得到的定理,因此也称为“孙子定理”。它是初等数论中最重要的基本定理之一,同时它刻画了剩余系的结构。这里根据中国剩余定理的思想方法编一个程序来解决两个问题,其中一是《孙子算经》里提出的问题,另外一个是著名的韩信点兵问题。

问题一 :“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”[4]。

此问题的程序如下：

```
#include "Stdio.h"
#include "Conio.h"
#include "math.h"
int main(void)
{
 long int m[3]={3,5,7},b[3]={2,3,2},E[3]={2,4,6};
 long int M[3], a [3],N[3];
 long int t,sum=0, x,i;
 t=m[0]*m[1]*m[2];
 for(i=0;i<3;i++)
 {
  M[i]=t/m[i];
  N[i]=pow(M[i],(E[i]-1));
   a [i]=N[i]%m[i];
   sum=sum+M[i]*b[i]* a [i];
   }
  x =sum%t;
  printf("%ld\n",sum);
  printf("%ld\n",y);
  }
```

运行结果：

```
SUM=233
 X=23
```

说明 :程序中的 E[0]=2,E[1]=4,E[2]=6 分别是3,5,7 的 *Euler* 函数,由“二”段的程序算出,也可以按“二”段的程序在上述程序中附加一个计算 Euler 函数的子程序或一个函数来完成。

问题二 :“有兵一队,若列成五行纵队,则末行一人 ;成六行纵队,则末行五人 ;成七行纵队,则末行四人 ;成十一行纵队,则末行十人,求兵数”[5]。(答 2111 人)

此问题的程序如下：

```
#include "Stdio.h"
#include "Conio.h"
int main(void)
{
 long  int  m [4]= {5,6,7,11},b [4]= {1,5,4,10},y [4]= {1,1,1,1};
 long int M[4],a[4],N[4],x[4],E[4];
 long int t,sum=0,i,X;
 t=m[0]*m[1]*m[2]*m[3];
 for(i=0;i<4;i++)
  {M[i]=t/m[i];
   E[i]=M[i]%m[i];
   while(y[i]%E[i]!=0)
   y[i]=y[i]+m[i];
   x[i]=y[i]/E[i];
   sum=sum+M[i]*b[i]*x[i];}
X=sum%t;
 printf("SUM=%ld\n",sum);
 printf("X=%ld\n",X);
 }
```

运行结果：

```
SUM=6731
 X=2111
```

说明 :在上述两个程序中求乘率时分别用到了同余式 $ax\equiv b(\mathrm{mod}m),(a,m)=1$ 的两种解法 :(1) $x\equiv b\cdot a^{\varphi(m)-1}(\mathrm{mod}m)$;(2) $x\equiv\frac{b}{a}(\mathrm{mod}m)$[6].虽然方法 (1) 要更公式化,但数 $a^{\varphi(m)-1}$ 容易超出 long int (长整型) 类型数的范围,所以在问题二中用了方法 (2) 。

5 Legendre 符号的计算

Legendre 符号是二次剩余理论的重要概念之

© 1994-2012 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net

一。通过 Legendre 符号的计算可以解决二次同余式是否有解的问题。而它的计算通常是利用二次反转定律 2 来计算,但是在计算过程中涉及符号上方的整数分解成标准分解式的问题。我们知道把一个整数分解成标准分解式是没有一般方法。因此,这里我用高斯引理[7]来编制程序。主要是用一个循环语句来进行计数,以此求 -1 的次数。

问题 求 Legendre 符号$\left(\frac{286}{563}\right)$的值。

```
#include "Stdio.h"
#include "Conio.h"
int main(void)
{ long int p,t=0,n,i,j,a,m,b;
printf("Input prime number:");
scanf("%ld",&p);
printf("Input integer:");
scanf("%ld",&n);
 j=(p-1)/2;
for(i=1;i<=j;i++)
 *{
  a=n*i;
  b=a%p;
  if(b>p/2)
  t=t+1;
  }
 {
  if(t%2!=0)
  m=-1;
  else m=1;
  }
printf("Legendre=%ld\n",m);
}
```

运行结果为:

```
Input prime number:563
 Input integer:286
 Legender=-1
```

说明 *程序段 * 的作用是先求$\frac{p-1}{2}$个不同的剩余类$n,2n,\cdots,\frac{p-1}{2}$的最小正剩余 然后算出它们中大于$\frac{p}{2}$的数的个数,即 -1 的次数。

参考文献

[1][7] 柯召,孙琦.数论讲义 (第二版) [M].北京:高等教育出版社, 2001.
[2][4][5] 闵嗣鹤,严士健.初等数论 (第三版) [M].北京:高等教育出版社, 2004.
[3] 潘承洞,潘承彪, 初等数论 (第二版) [M].北京:北京大学出版社,2003.
[6] 李复中.初等数论选讲[M].吉林:东北师范大学出版社, 1984.
[8] 谭浩强.C 程序设计[CP].北京:清华大学出版社,1991.

The application of computer program languages in Elementary Number Theory

Duobu Jie
(Department of Mathematics, Tibet University, Lhasa 850000, China)

Abstract: Number Theory is related closely to the informatics´ generation along with developing electronic computers. It is not only apparent to the application of Number Theory in the Computers, but also apparent to the important influence in the techniques of the computers and the domain of the network. Particularly, the naissance of the computer program languages is the cogent tool to study of Number Theory. This paper mainly introduces the applications of the computer program languages to Number Theory problems such as the standard decomposition of , Euler function, Chinese residual Theorem, and the Legendre symbols etc.

Key words: C language; elementary Number Theory; application; Euler function; Chinese residual Theorem

[责任编辑 :肖干田]

© 1994-2012 China Academic Journal Electronic Publishing House. All rights reserved. http://www.cnki.net