基于 Maple 的原根及本原多项式的计算*

程 瑶,李 杨,李世奇
(重庆师范大学 数学与计算机科学学院,重庆 400047)

摘 要:在数论中,求解整数的原根和多项式的本原多项式是比较复杂的问题。本文应用 Maple 数学软件给出了求解它们的通用程序,大大的简化了此类问题的计算。例证表明 Maple 在计算原根和本原多项式的有效性。

关键词:原根;本原多项式;程序设计
中图分类号:O156.1;O245 **文献标识码**:A **文章编号**:1672-6693(2005)02-0027-03

The Appliance of Maple in Primitive Root and Primitive Polynomia

CHENG Yao, LI Yang, LI Shi-qi
(College of Mathematics and Computer Science, Chongqing Normal University, Chongqing 400047, China)

Abstract: How to solve the primitive root of integers and the primitive polynomial of polynomial are complex problems in number theory. We give algorithm of the Maple by using the continued fraction and also get the general programs. The calculation can be simplified largely. In addition, this paper gives some examples to prove the efficiency of Maple in the aspect of solving the primitive root and primitive polynomial.

Key words: primitive root; primitive polynomial; program design

Maple 是当今国际上广泛应用的计算机代数系统,该数学软件系统对数论中的数值的计算和符号的处理提供了强大的计算功能,有不少文献对其进行了不同方面的论述[1~3]。事实上,该软件专门提供了有关数论的软件包,其中有对数论中常用的数值计算行之有效的工具,例如有如下标准处理函数[4,5],index(mlog):求 $a^y \equiv x \pmod n$ 中的 y,即指数;invphi:求欧拉函数 $\varphi(n)$;mcombine:孙子剩余定理;mroot:求模的根,即求满足的 $y^r \equiv x \pmod p$ 的 y;msqrt:求模的平方根,即求满足 $y^2 \equiv x \pmod p$ 的 y;order:次数;phi:计算欧拉函数;pi:计算不大于给定的一个正整数 n 的素数的个数;primroot:计算最小的原根;rootsunity:求单位根。

1 Maple 关于数论的简单应用

1.1 欧拉函数 $\varphi(a)$ 的计算方法[6]

例 1 设 $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$,则

$$\varphi(a) = a\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)。$$

对于简单的 a 容易计算,但是当 a 很大时,计算就很困难了,这时就可以用 Maple 中所提供的 the numtheory package 中的 phi 来求值了。

解 > with(numtheory):

> phi(180);

最后得到计算结果为 48。

1.2 计算次数的方法[7]

设整数 a 满足 $(a,m)=1, m>0$,a 对模 m 的次数为 l。因为 $l \mid \varphi(m)$,故次数 l 可通过计算 $a^{d_1}, a^{d_2}, \cdots, a^{d_s}$ 模 m 的值求出,这里 $d_1, d_2, \cdots, d_s$ 是 $\varphi(m)$ 的诸因子。

定理 1 如果是 $m = p_1^{l_1} \cdots p_k^{l_k}$ 是 m 的标准分解式,整数 a 对模 m 的次数等于整数 a 对模 $p_i^{l_i}$ $(i=1, \cdots, k)$ 的诸次数的最小公倍数。

例 2 设 $a=2, m=45=5\times 9$,2 对模 5 的次数是 4,2 对模 9 的次数是 6,故 2 对模 45 的次数为 [4,

* 收稿日期:2004-11-16 修回日期:2005-04-25
资助项目:重庆市教委科研基金项目
作者简介:程瑶(1981-),女,沈阳人,硕士研究生,主要研究方向为数论。

6] = 12。

解 > with(numtheory):

> order(2,45);

最后得到计算结果为12。

定理2 设 p 是一个素数,a 对模 p^j 的次数是 f_j,则 $f_{j+1}=f_j$ 或 $f_{j+1}=pf_j$。又设 $p^j \| a^{f_2}-1$,进而有

$$f_j=\begin{cases} f_2, & \text{如果 } 2\leqslant j\leqslant i \\ p^{j-i}f_2, & \text{如果 } j>i \end{cases}$$

例3 设 $a=7$,$p=2$,求7对模 2^{10} 的次数 f_{10}。因为 $f_1=1$,$f_2=2$,且 $7^2-1=48$,$2^4 \| 48$,故

$$f_{10}=2^{10-4}\cdot 2=2^7=128$$

解 在Maple中,计算次数,输入

> with(numtheory):

> order(7,2^10);

得到计算结果:128。

Maple提供的数论软件包并不能解决所有的数论问题,但是Maple提供了Maple程序设计语言,从而把软件包与Maple语言结合可以解决更多的数论问题。

2 原根的计算方法和原理

例4 求模 m 的原根,即求满足 $a^{\varphi(m)}\equiv 1 \pmod m$ 的 a 的值。

有文献给出了计算原根的方法如下[7]。

设 $(g,m)=1$,$m=p^l$ 或 $2p^l$,p 是一个奇素数,判断 g 是否是 m 的原根,不需要逐一计算 $g^1,g^2,\cdots,g^{\varphi(m)-1}$,而只需计算 $g^t \pmod m$,这里 $t/\varphi(m)$。基于这样的想法,有下面的定理。

定理3 设 $m>2$,$\varphi(m)$ 的所有不同的素因子是 $q_1,q_2,\cdots,q_s$,$(g,m)=1$,则 g 是 m 的一个原根的充分必要条件是 $g^{\frac{\varphi(m)}{q_i}}$ 与1不同模于 m,$(i=1,2,\cdots,s)$。

定理4 设 a 对模奇素数 p 的次数是 d,$d<p-1$,则 $a^\lambda(\lambda=1,2,\cdots,d)$ 都不是 p 的原根。

例5 求出41的原根。

通常的算法是先列出1,2,3,…,40。因为2对模41的次数为20,列出的数中除去以下各数2,4,8,16,32,23,5,10,20,40, 39,37,33,25,9,18,36,31,21,1。其次取3,因为3对模41的次数是8,因此在所列的数中除去3,9,27,40,38,32,14,1,其中1,9,32,40第一次已除去,则在 $\varphi(40)$ 中还剩下6,7,11,12,13,15,17,19,22, 24,26, 28,29,30,34,35这些数,它们都是41的原根。

下面用Maple中the numtheory package的order设计一个程序来求原根。

解 > m:=proc(p)

> global a,y;

> with(numtheory);

> for a do

> y:=order(a,p);

> if (y=p-1) and (a<p) then print(a) fi;if (a=p) then break fi;

> od;

> end;

利用这个程序求41的原根,输入

> m(41):

结果是

6 7 11 12 13 15 17 19
22 24 26 28 29 30 34 35

3 本原多项式的计算方法

F_2 上的 n 次本原多项式在代数编码中非常有用,可以通过分解 $F^{2^n-1}(x)$ 来求得,但比较困难。在代数里有一些专门的方法来求一个本原多项式,如果知道了一个本原多项式可以通过有限域的性质一一求出。对于求任意数域上的 n 次本原多项式更为困难。

例6[7] 已知多项式 x^4+x^3+1 是 F_2 上的一个4次本原多项式,它的一个根 $\alpha\in F_{2^4}$,是一个原根,于是 F_{2^4} 的16个元可以表示为 $0,1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}$。由于 $\frac{\varphi(15)}{4}=2$,故还有一个四次本原多项式。

通常的解法是先计算出 x^4+x^3+1 的4个根为 α、α^2、α^4、α^8,再由 α^7 的阶是15,求出 α^7 的极小多项式 $m(x)$,这样,也就求出了另一个 F_2 上的四次本原多项式。

解法1 (通常解法)令 $u=\alpha^7$,它的极小多项式为 $m_1(x)=a_0+a_1x+a_2x^2+a_3x^3+a_4x^4$,由 $1=1$,$u=\alpha^7=1+\alpha+\alpha^2$,$u^2=\alpha^2+\alpha^3$,$u^3=1+\alpha+\alpha^2+\alpha^3$,$u^4=\alpha+\alpha^2$,易知 $m(x)$ 的系数适合方程

$$(a_0,a_1,a_2,a_3,a_4)\begin{pmatrix}1&0&0&0\\1&1&1&0\\0&0&1&1\\1&1&1&1\\0&1&1&0\end{pmatrix}=(0,0,0,0)$$

此方程有解(1,1,0,0,1),即 $m_1(x)=x^4+x+1$。

而在 Maple 中,则可以设计一个程序,使得如果任意给出一个素数 p,且指定次数 n,能求出所有次数为 n 的 F_p 上的本原多项式。

解法 2　先设计 Maple 程序如下

```
> restart:
> K:=proc(p,nnum)
> global f,d,a,ymove,temppoint,ytemp,xtemp,i,j;
> f:=0;
> for i from 0 to nnum do f:=a[i]*X^i+f;od;
> ymove:=1;temppoint:=1;
> for i from 0 to nnum do
> ymove:=ymove*p;od;
> for ytemp from 1 to ymove do
> for xtemp from 0 to nnum do
> temppoint:=1;
> if ((nnum-xtemp)>0) then
> for i from 1 to nnum-xtemp do temppoint:=temppoint*p;od;
> a[xtemp]:=iquo(ytemp,temppoint) mod p;
> else a[xtemp]:=ytemp mod p;fi;
> subs(a[xtemp]=a[xtemp],f);od;d:=Primitive(f) mod p;if(d='true') and (a[nnum]<>0) then print(f) fi;
> od;
> end;
```

应用上述程序后,给定一个素数 2,且指定次数 4,求所有次数为 4 的 F_2 上的本原多项式。

先输入　　`> K(2,4);`

得到如下结果

$$X^4+X^3+1$$

$$X^4+1+X$$

这样就可以随意的求出本原多项式了。

参考文献:

[1] 李世奇. 应用 Maple 研究四元数和四元群[J]. 重庆师范学院学报(自然科学版),2000,17(2):41-45.

[2] 李世奇. 计算机代数系统 MAPLE 及其程序设计语言[J]. 重庆师范学院学报(自然科学版),1998,15(4):78-84.

[3] 冯国锋. 广义中国剩余定理及其 Maple 解法[J]. 重庆师范大学学报(自然科学版),2004,21(3):5-7.

[4] 科学出版社名词室. 新英汉数学词汇[M]. 北京:科学出版社. 2002.

[5] 李世奇. Maple 6 计算机代数系统应用及程序设计[M]. 重庆:重庆大学出版社. 1999.

[6] 闵嗣鹤,严士健. 初等数论[M]. 北京:高等教育出版社. 1982.

[7] 柯召,孙琦. 数论讲义(上、下)[M]. 北京:高等教育出版社. 1986.

(责任编辑　黄　颖)