文章编号:1005－0523(2003)04－0103－03

方程 $1+x+\cdots+x^n=0 \pmod p$ 的解与算法

周尚超

(华东交通大学 学报编辑部,江西 南昌 330013)

摘要:给出了方程 $1+x+\cdots+x^n=0 \pmod p$ 的解与算法.

关 键 词:同余方程;初等数论;积性函数;循环群
中图分类号:O156.1　　**文献标识码**:A

本文的数均为整数且 p, q, r, s 表示素数,(m, n)是 m 和 n 的最大公因数. $\sigma(n)$是 n 的因子(含 1 和 n)之和, 例如 $6=1+2+3+6=12$. σ 是积性函数,即 $(m, n)=1$, 则 $\sigma(mn)=\sigma(m)\sigma(n)$. 文献[1],[2]给出如下定理:

定理 1[1,2]　设

$f(x)=a_n x^n+a_{n-1}x^{n-1}+\cdots+a_1 x+a_0$, $n>0$, $a_n\not\equiv 0 \pmod p$,

是一个多项式. 则同余方程

$$f(x)=0 \pmod p \tag{1}$$

最多有 n 个解.

本文研究同余方程

$$1+x+\cdots+x^n=0 \pmod p,\ n>1 \tag{2}$$

的解与算法. 得到定理 2,3,4,它们在计算数的因子和或数的素数因子方面有用.

令 n 的标准分解式为:$n=p^a q^b\cdots s^k$. 则

$$\sigma(n)=\sigma(p^a)\sigma(q^b)\cdots\sigma(s^k)$$

而　$\sigma(r^j)=1+r+r^2+\cdots+r^j$

数的因子和的计算,可化为数的素数因子的计算. 在我们的 1 个较大的计算项目中,需要计算 $1+r+r^2+\cdots+r^n$ 的标准分解式. 就是要计算它的素因子. 这就需要求解方程(2).

例　$r=76123$, $\sigma(r^4)=33579118185146514761$

$\sigma(r^4)=11*151*1721*16001*19571*37511$

计算 $\sigma(r^4)$的素因子,要用$\leqslant\sigma(r^4)$的平方根的素数去试除 $\sigma(r^4)$,计算量是巨大的. 从本例可知 $\sigma(r^4)$的素因子 $p=1 \pmod 4$. 如是则计算量减少到原来的 1/4.

定义 1　欧拉函数 $\varphi(n)$的值等于 $1, 2, \cdots, n-1$ 中与 n 互素的数的个数.

对于素数 p, $\varphi(p)=p-1$.

定义 2　设 m 是使

$$b^m=1 \pmod p$$

成立的最小正整数,则 m 叫做 b 对模 p 的次数

定义 3　次数是 $p-1$ 的数叫做 p 的原根

引理 1[2]　设 $m>1$, $(b, m)=1$, 则

$$b^{\varphi(m)}=1 \pmod m$$

引理 2[2]　设 $a\not\equiv 0 \pmod p$, 则

$$a^{p-1}=1 \pmod p$$

引理 3[2]　设 a 对模 p 的次数是 m, $a^n=1 \pmod p$ 则 $m \mid n$.

定理 2　设 $p>n+1$, b 是 p 的 1 个原根, $n+1$ 是素数,则(2)有解的充分必要条件是

$$p=1 \pmod{n+1}$$

且当有解时, $a, a^2, \cdots, a^n$ 是(2)的 n 个解. 这里 $a=b^k \pmod p$, $k=(p-1)/(n+1)$.

证明　充分性. 设 $p=1 \pmod{n+1}$, $k=(p-1)/(n+1)$. $a=b^k \pmod p$, $a\not\equiv 1 \pmod p$, $a^{n+1}=1 \pmod p$

收稿日期:2003－01－10
作者简介:周尚超(1948－),男,云南蒙自人,教授.

$1+a+\cdots+a^n+a^{n+1}$

$=1+a+\cdots+a^n+1(\mathrm{mod}\ p)$

$=(1+a+\cdots+a^n)a+1(\mathrm{mod}\ p)$

$1+a+\cdots+a^n=(1+a+\cdots+a^n)a\ (\mathrm{mod}\ p)$

$(a-1)(1+a+\cdots+a^n)=0\ (\mathrm{mod}\ p)$

$1+a+\cdots+a^n=0(\mathrm{mod}\ p)$

a 是(2)的解.

必要性. 设 $1+a+\cdots+a^n=0\ (\mathrm{mod}\ p)$. 易知 $a\neq 1\ (\mathrm{mod}\ p)$

$1+a+\cdots+a^n+a^{n+1}$

$=(1+a+\cdots+a^n)a+1\ (\mathrm{mod}\ p)$

$a^{n+1}=1\ (\mathrm{mod}\ p)$

若 $1<h<n+1$, $a^h=1(\mathrm{mod}\ p)$, 由引理 3, $h\mid n+1$, 不可. 由引理 3, $n+1$ 整除 $p-1$. $p=1(\mathrm{mod}\ n+1)$. $1,2,\cdots,p-1$ 在 mod p 乘法下是 $p-1$ 阶循环群, a 生成 $n+1$ 阶子群 $<a>$, $n+1$ 是素数, $<a>$ 是素数阶循环群, $<a>$ 中任何非单位元的元素的阶是 $n+1$, 即 $<a>=<a^2>=\cdots=<a^n>$. $a, a^2, \cdots, a^n$ 是(2)的 n 个解.

推论 设 $p>n+1$, $n+1$ 是素数. 若 h 是方程(2)的解, 则方程(2)的所有解是 $h, h^2, \cdots, h^n$

定理 3 设 $p=n+1$, 则(2)有唯一解 $x=1(\mathrm{mod}\ p)$

证明 显然 $x=1(\mathrm{mod}\ p)$ 是解. 设 $x\neq 1(\mathrm{mod}\ p)$. $x^n=1(\mathrm{mod}\ p)$. 由定理 2 必要性的证明, 得

$1+x+\cdots+x^{n-1}=0(\mathrm{mod}\ p)$

$1+x+\cdots+x^{n-1}+x^n=1(\mathrm{mod}\ p)$

x 不是解.

定理 4 设 $p<n+1$, $n+1$ 是素数, 则(2)无解

证明 显然 $x=1(\mathrm{mod}\ p)$ 不是解. 设 $x\neq 1(\mathrm{mod}\ p)$. 则 $x^{p-1}=1(\mathrm{mod}\ p)$, 设 t 是 x 的次数, $x^t=1(\mathrm{mod}\ p)$ 的最小值, 则 $1<t\leqslant p-1$, 设 $n+1=kt+h$, $h<t$. 由定理 2 必要性的证明, 得

$1+x+\cdots+x^{t-1}=0(\mathrm{mod}\ p)$

而对 $h<t$

$1+x+\cdots+x^{h-1}\neq 0(\mathrm{mod}\ p)$

$1+x+\cdots+x^{n-1}+x^n=(1+x+\cdots+x^{t-1})(1+x^t+x^{2t}+\cdots+x^{(k-1)t})+x^{kt}(1+x+\cdots+x^{h-1})(\mathrm{mod}\ p)$

$=x^{kt}(1+x+\cdots+x^{h-1})(\mathrm{mod}\ p)$

$=(1+x+\cdots+x^{h-1})(\mathrm{mod}\ p)$

$\neq 0(\mathrm{mod}\ p)$

x 不是解. (2)无解.

设 $n+1$ 不是素数. $n+1=kt$, t 是素数, 则

$1+x+x^2+\cdots+x^n=(1+x+\cdots+x^{t-1})(1+x^t+x^{2t}+\cdots+x^{(k-1)t})$

先解 $1+x+\cdots+x^{t-1}=0(\mathrm{mod}\ p)$, 再解 $(1+x^t+x^{2t}+\cdots+x^{(k-1)t})=0(\mathrm{mod}\ p)$.

如 k 是素数, 则先求得 $1+x+\cdots+x^{k-1}=0(\mathrm{mod}\ p)$ 的解 $x=a$, 再求

$x^t=a(\mathrm{mod}\ p)$ 的解. 如 k 不是素数, 则重复以上过程求解.

例 1 $p=31$, 解方程

$1+x+x^2+x^3+x^4=0\ (\mathrm{mod}\ p)$ (3)

由定理 2, $p=31=1\ (\mathrm{mod}\ 5)$, $k=6,3$ 是 p 的原根. $a=3^6=16(\mathrm{mod}\ p)$. (3)的 4 个解是 $a=16$, $a^2=8$, $a^3=4$, $a^4=2\ (\mathrm{mod}\ p)$.

例 2 $p=13$, 解方程

$1+x+x^2+\cdots x^{26}=0\ (\mathrm{mod}\ p)$ (4)

$1+x+x^2+\cdots x^{26}$

$=(1+x+x^2)(1+x^3+x^6)(1+x^9+x^{18})$

$x=3$, $x=9$ 是方程 $1+x+x^2=0(\mathrm{mod}\ p)$ 的解. $x^3=3,9\ (\mathrm{mod}\ 13)$ 无解. (4)的解是 $x=3,9\ (\mathrm{mod}\ p)$.

例 3 $p=31$, 解方程

$1+x+x^2+\cdots x^{14}=0\ (\mathrm{mod}\ p)$ (5)

$1+x+x^2+\cdots x^{14}$

$=(1+x+x^2)(1+x^3+x^6+x^9+x^{12})$

$x=5$, $x=25$ 是方程 $1+x+x^2=0(\mathrm{mod}\ p)$ 的解. 由例 1(3)的解集是 $\{2,4,8,16\}$. 令 $a\in\{2,4,8,16\}$, $x^3=a(\mathrm{mod}\ p)$ 的解集仍为 $\{2,4,8,16\}$. 因此(5)的解集为 $\{2,4,8,16\}(\mathrm{mod\ p})$.

以下讨论算法和程序.

定理 5[2] 设 b 对模奇素数 p 的次数是 m, $m<p-1$, 则

$b^k, k=1,2,\cdots,m$

都不是 p 的原根

当 $n+1$ 为素数且 $p-1=k(n+1)$ 时方程(2)的 n 个解 $x[1],\cdots,x[n]$ 算法.

程序中 $h[m]=b^m$, 算到 $b^m=1\ (\mathrm{mod}\ p)$ 为止. 如果 $m=n+1$, 则 $x[1]=b,\cdots,\ x[n]=b^n$. 跳出 b 循环(break). 如果 $m=p-1$, 即 $b^{(p-1)}=1$, b 是 p 的原根, $a=b^k$. $x[1]=a,\cdots,\ x[n]=a^n$. 跳出 i 循环(break). 如果 $m\neq p-1$, $m\neq n+1$. 根据定理 5 和推论, $h[j], j=1,2,\cdots,m$ 都不是 p 的原根也不是解, 对这些数标记为 $f[h[j]]=1$, 不在进行计算, 以提高计算效率.

```
x[0]:=1;
for j:=1 to p do f[j]:=0;
```

```
for b:=2 to p-1 do begin
  if f[b]:=1 then continue;
  m=1;h[m]:=b;
  while h[m]<>1 do begin
    h:=h * b mod p;
    m:=m+1;
  end;
  if m=n+1 then begin
    for j:=1 to n do x[j]:=x[j-1] * b mod p;
    break;
  end;
  if m=p-1 then begin
    a:=b;
    for j:=2 to k do a:=a * b mod p;
    for j:=1 to n do x[j]:=x[j-1] * a mod p;
      break;
  end;
  for j:=1 to m do f[h[m]]:=1;
end;
```


参考文献:

[1] 柯召,孙琦. 数论讲义[M]. 北京:高等教育出版社,1987.

[2] 华罗庚. 数论导引[M]. 北京:科学出版社,1979.

[3] 曹珍富. 数论中的问题与结果[M]. 哈尔滨:哈尔滨工业大学出版社,1996.

The Algorithm and Programming of $1+x+\cdots+x^n=0(\mathbf{mod}\ p)$

ZHOU Shang-chao

(Editorial Board of Journal, East China Jiaotong Univ., Nanchang 330013 China)

Abstract: The Algorithm and Programming of $1+x+..+x^n=0(\mathrm{mod}\ p)$ is given in this paper.

Key words: equation of congruence; elementary thery of numberbs; multiplicative function; cyclic group