《初等数论》中的模 p 法及其应用

方　辉,方　炜
(黄山学院 数学系,安徽 黄山 245041)

摘　要:利用模 P(或 P 的方幂)法,结合数论中关于素数 P 的基本性质和结论,有效的讨论了同余式,整系数多项式,整系数矩阵,群的阶等问题。

关键词:素数;同余;模 P 法;二次互反律
中图分类号:0156　　**文献标识码**:A　　**文章编号**:1672-447X(2009)03-0023-05

0 引　言

《初等数论》中同余的概念不是从 *Gauss* 开始的，它最早出现在 *Euler*,*Lagrange* 和 *Legendre* 的著作中,但是 *Gauss* 在《算术探究》这部伟大的作品中第一节引进了同余的记号 $a\equiv b(modm)$并随后讨论了同余的基本性质及其应用,从而完整的建立了同余理论。

我们知道数论中的素数就如物理学中的基本粒子或类似于化学中的元素的地位,其重要性自不待言。关于自然数 a 有以下两种基本表示:

(Ⅰ)整数环 Z 上的唯一分解定理:$a=p_1^{\alpha 1}p_2^{\alpha 2}\cdots p_s^{\alpha s}$,其中 $p_1,p_2\cdots,p_s$,为互异素数;

(Ⅱ)p 进制表示:$a=d_0+d_1p+\cdots+d_kp^k$ 其中 p 是素数且 $0\le d_i\le p-1,i=1,2,\cdots k$。

我们知道在 (Ⅰ)$p_1,p_2\cdots,p_s$ 中包括了所有能整除 a 的素数,因此,它由 a 唯一决定。同样,指数 $\alpha_1,\alpha_2,\cdots,\alpha_s$ 也由 a 唯一确定。(Ⅱ)中给定一个素数 p,$d_0,d_2,\cdots,d_k$ 及 k 都由 a 唯一确定。

文献[1]在丢番图方程求解上应用模 p(或 p 的方幂)法,解决许多丢番图方程问题。本文讨论模 p(或 p 的方幂)法在以下问题中的应用。

所谓模 p(或 p 的方幂)法,指关于整数的命题(含丢番图方程,整系数多项式,整系数矩阵,群的阶等问题),通过模素数 p(或 p 的方幂)进行计算,判定命题正确与否的方法。本文中的字母 a,b,c 都表示整数。

1　初等数论中的应用

1.1　最大公因数问题

命题 1　$(a,b)=1\Leftrightarrow b$(或 a)的任意一个素因子 p,都有 $a\not\equiv 0(modp)$或 $b\not\equiv 0(modp)$。

证明:假设 $(a,b)\neq 1$,设 p 是 a,b 的一个素因子,可得到模 p 的一个矛盾式。故命题 1 成立。

例 1[2] 设 m,n 为正整数,且 m 是奇数,则$(2^m-1,2^n+1)=1$。

证明:假设$(2^m-1,2^n+1)\neq 1$,则存在$(2^m-1,2^n+1)$的一个素因子 p,又因为 m 是奇数,可得:

$$2^m\equiv 1(\mathrm{mod}p)\Rightarrow 2^{mn}\equiv 1(\mathrm{mod}p) \quad (1)$$

$$2^m\equiv -1(\mathrm{mod}p)\Rightarrow 2^{mn}\equiv -1(\mathrm{mod}p) \quad (2)$$

(1)与(2)不符,故结论成立。

收稿日期:2008-10-26
基金项目:安徽省教育厅教学研究基金资助(2007jyxm113)
作者简介:方　辉(1963-),安徽休宁人,黄山学院数学系副教授,研究方向为代数与数论;
方　炜(1975-),安徽歙县人,黄山学院数学系讲师,研究方向为典型群与代数。

例 2[2] 设$(a,b)=1$,$a+b\neq 0$,且 p 是一个奇素数,则:$(a+b,\frac{a^p+b^p}{a+b})=1$ 或 p。

证明:若$(a+b,\frac{a^p+b^p}{a+b})\neq 1$,设 q 是$(a+b,\frac{a^p+b^p}{a+b})$的任意一个素因子,$q^k \parallel (a+b,\frac{a^p+b^p}{a+b})$(即 $q^k \mid (a+b,\frac{a^p+b^p}{a+b})$,但 $q^{k+1}\nmid(a+b,\frac{a^p+b^p}{a+b})$),则 $\frac{a^p+b^p}{a+b}=\frac{(a+b-b)^p+b^p}{a+b}\equiv(a+b)^{p-1}+\binom{p}{1}(a+b)^{p-2}(-b)+\cdots+\binom{p}{p-1}(-b)^{p-1}\equiv pb^{p-1}\equiv 0(\mathrm{mod}\,q^k)$,由于$(a,b)=1\Rightarrow(b,a+b)=1\Rightarrow(b,q)=1$,即$(b^{p-1},q^k)=1$,于是 $p\equiv 0(\mathrm{mod}q^k)$,因为 p,q 是素数,所以 $p=q$,及 $k=1$,再由 q 的任意性可知 $(a+b,\frac{a^p+b^p}{a+b})=p$。

1.2 同余方程 $a^b\equiv x(\mathrm{mod}n)$求解问题

求上面同余方程的方法很多,但对 a,b,n 都很大时,计算还是比较困难。下面用模 p 法和孙子定理结合给出一种算法。

命题2 设$(a,n)=1$,$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$,$m_i=\frac{n}{p_i^{\alpha_i}}$,$i=1,2,\cdots$,由于 $a^b\equiv x_i(\mathrm{mod}\,p_i^{\alpha_i})$,$i=1,2,\cdots,s$,

$m_im_i'\equiv 1(\mathrm{mod}\,p_i^{\alpha_i})$,$i=1,2,\cdots,s$,

则:$x\equiv a^b\equiv\sum_{i=1}^{s}m_im_i'x_i(\mathrm{mod}\,n)$ (3)

注:为了计算方便,上面的计算过程中常常结合 *Euler-Fermat Theorem*。

定理 如果$(a,n)=1$,则 $a^{\varphi(n)}\equiv 1(\mathrm{mod}\,n)$ (4)

特别地 $a^{p^{\alpha_i-1}(p-1)}\equiv 1(\mathrm{mod}\,p^{\alpha_i})$ (5)

$a^{p-1}\equiv 1(\mathrm{mod}\,p)$ (6)

(6)式又称为 *Fermat's Little Theorem*。

例 3 求 123^{456} 的最后两位数。

解: 原问题等价于 $123^{456}\equiv x\ (mod100)$,因为 $100=2^2\times5^2$,$2^{\varphi(25)}=2^{20}\equiv 1\ (mod5^2)$,则 $123^{456}\equiv 1\ (mod2^2)$,$123^{456}\equiv(-2)^{456}\equiv 11\ (mod5^2)$

$25m_1'\equiv 1\ (\mathrm{mod}2^2)\Rightarrow m_1'\equiv 1$ $4m_2'\equiv 1\ (mod5^2)\Rightarrow m_2'\equiv -6$,$x\equiv 123^{456}\equiv 25+11\times4\times(-6)\equiv 61\ (mod100)$,所以 123^{456} 的最后两位数为 61。

例 4 若 2008^m 与 $2008^n(m>n>0)$的最后三位数字相同,试求 m,n,使 $m+n$ 的值最小。

解: 依题意有 $2008^m\equiv 2008^n(\mathrm{mod}1000)$,即 m,n 同时满足:(ⅰ)$2008^m\equiv 2008^n(\mathrm{mod}2^3)$;

(ⅱ)$2008^m\equiv 2008^n(\mathrm{mod}5^3)$

在(ⅰ)中由于 $8\mid 2008\Rightarrow m-n\geq 1$,及 $n>0$ 知 n 的最小值为 1。在(ⅱ)中 $2008=8\times251$,$(2008,5^3)=1$ 则(ⅱ)等价于 $8^{m-n}\equiv 1(\mathrm{mod}5^3)$ (7)

由(5)式知 $8^{25(5-1)}\equiv 1(\mathrm{mod}5^3)$,及 m,n 取最小值,可得 $m-n\mid 100$,再由(7)知 $8^{m-n}\equiv 1(\mathrm{mod}5)$以及 $8^4\equiv 1(\mathrm{mod}5)$。则 $m-n$ 只能取 4,20,100 三数之一,$8^4\equiv 96(\mathrm{mod}5)$,$8^{20}\equiv 101(\mathrm{mod}5)$,故 $m-n=100$,m 的最小值为 101,所以$(m+n)_{min}=102$。

注:关于同余方程:$f(x)=\sum_{i=0}^{k}a_ix^i\equiv 0(\mathrm{mod}\,n)$ (8)

其中 $a_i\in N$,$i=0,1,2,\cdots,k$,$n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$,$p_i$ $(i=1,2\cdots,s)$为互异的素数。我们也可以用同样的方法求解,《初等数论》教材中都有,这里不再举例。

1.3 奥林匹克数学竞赛问题

在省级以上的奥林匹克数学竞赛中,一般都会有数论问题,尤其国家和 *IMO* 试题中,数论是必考的内容。

中学新教材把初等数论初步放在选修内容中,充分说明了《初等数论》这门课程的重要性,我们完全可以预测不久将会在高考中出现初等数论试题。

例 5 求出所有大于 1 的整数 n,使得 $\frac{2^n+1}{n^2}$ 是一个整数。

解: 设 p 是奇数 n 的最小素因子,则 $2^n\equiv -1(\mathrm{mod}p)$,而 a 是满足 $2^a\equiv -1(\mathrm{mod}p)$的最小正整数,易得 $a\mid n$。若 $a>p-1$,有 $a-(p-1)<p$ 及费马小定理 $2^{p-1}\equiv 1(\mathrm{mod}p)$,可得 $2^{a-(p-1)}\equiv -1(\mathrm{mod}p)$与 a 的取法矛盾,故 $1\leq a\leq p-1$,由 p 是 n 的最小素因子及 $a\mid n$ 知 $a=1$,$2^1\equiv -1(\mathrm{mod}p)$推出 $p=3$。

原问题等价于求丢番图方程:$2^x+1=yx^2$ 的全部非平凡正整数解。上式左边是奇数,故 x 是奇数。可得 $2^x+1\equiv(-1)^x+1\equiv 0(mod3)$,设有正整数 k 使得 $3^k\parallel x$(即 $3^k\mid x$,但 $3^{k+1}\nmid x$),则有 $2^x\equiv -1(\mathrm{mod}3^{2k})$,可得 $2^{2x}\equiv 1(\mathrm{mod}3^{2k})$。由(5)式知:$2^{2\cdot3^{2k-1}}\equiv 1(\mathrm{mod}3^{2k})$,而由数学归纳法可知:$2^{3^{2k-1}}\equiv -1(\mathrm{mod}\,3^{2k})$,则 2 是模 3^{2k} 的原根,故有 $2x=2\cdot3^{2k-1}\Rightarrow k=2k-1$,即 $k=1$,所以 $x=3$,$y=1$ 是方程的解。

于是大于 1 的整数 n 只有 3。

例 6[3] 证明如果 $2n+1$,$3n+1$ 都是完全平方数,

则 n 能被 40 整除。

证明：我们只需证明 $n\equiv 0(\mathrm{mod}5), n\equiv 0(\mathrm{mod}8)$ 即可。由于 $2n+1$ 是奇数又是完全平方数，则 $2n+1\equiv 1(\mathrm{mod}8)\Rightarrow n\equiv 0(\mathrm{mod}4)$，可得 $3n+1$ 也是奇数且为完全平方数，则 $3n+1\equiv 1(\mathrm{mod}8)$，$(3,8)=1$，从而有 $n\equiv 0(\mathrm{mod}8)$。注意到平方数模 5 的余数必定是 0,1,-1 之一，由于 $2n+1+3n+1\equiv 2(\mathrm{mod}5)\Rightarrow 2n+1\equiv 1(\mathrm{mod}5), 3n+1\equiv 1(\mathrm{mod}5)$ 则 $n=3n+1-(2n+1)\equiv 0(\mathrm{mod}5)$，故 n 能被 40 整除。

例 7　设 n 不是完全平方数，证明：$\sqrt{n}+\sqrt{n+1}$ 是无理数。

证明：假设 $\sqrt{n}+\sqrt{n+1}$ 是有理数 r，则 $\sqrt{n+1}-\sqrt{n}=\frac{1}{r}$，可得 $\sqrt{n}=\frac{1}{2}(r-\frac{1}{r})$ 为有理数。我们只需证明 $\sqrt{n}$ 是无理数。假设 $\sqrt{n}$ 是有理数，设 $\sqrt{n}=\frac{a}{b}, a,b\in\mathbb{Z},\ b\neq 0\Rightarrow nb^2=a^2$，由 n 不是完全平方数，设 p 是 n 素因子且最高次数为奇数，s,t 分别为 nb^2, a^2 中 p 的指数，从而有 $1\equiv s\equiv t\equiv 0(\mathrm{mod}2)$，矛盾。故是 $\sqrt{n}$ 无理数。

2　其它课程中的应用

2.1　判定整系数矩阵的可逆性问题

设 $A=\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}$ 是一个整系数矩阵（即 $a_{ij}\in\mathbb{Z}\ \ i,j=1,2,\cdots,n$ ），p 是一个素数。定义：

$$\begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{pmatrix}(\mathrm{mod}\,p)=\begin{pmatrix} a_{11}(\mathrm{mod}\,p) & a_{12}(\mathrm{mod}\,p) & \cdots & a_{1n}(\mathrm{mod}\,p) \\ a_{21}(\mathrm{mod}\,p) & a_{22}(\mathrm{mod}\,p) & \cdots & a_{2n}(\mathrm{mod}\,p) \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1}(\mathrm{mod}\,p) & a_{n2}(\mathrm{mod}\,p) & \cdots & a_{nn}(\mathrm{mod}\,p) \end{pmatrix}$$

记上式右端的矩阵为 A_p，则有下面的结论：

命题 3　若 $\det A_p\not\equiv 0(\mathrm{mod}\,p)\Rightarrow \det A\neq 0$。

命题 3 告诉我们对一个整系数方阵判定其可逆性，如果选取一个素数 p，使得 $detA_p\neq 0$，则可以判定 A 方阵是可逆的。文献[4]有下面的问题。

例 8[4]　设 $2n+1$ 个数 $a_1,a_2,\cdots a_{2n+1}\in C$ 满足如下条件：任意从这 $2n+1$ 个数中去掉一个，则可以将余下的 $2n$ 个数分成两组，每组 n 个，使得两组数相等。证明这 $2n+1$ 个数相等。(1973 年 *Putnam Exam*)

证明：对每个 i，去掉 a_i 后剩下的 $2n$ 个数满足关系式：

$$a_{i_1}+a_{i_2}+\cdots+a_{i_n}=a_{i_{n+1}}+a_{i_{n+2}}+\cdots+a_{i_{2n}}$$

其中 $i_1,i_2,\cdots,i_{2n}$ 为 $1,2,\cdots,i-1,i+1,\cdots,2n+1$ 的一个排列。将上式改写

$$\sum_{j=1}^{2n+1}c_{ij}a_j=0\ \ i=1,2,\cdots,2n+1. \tag{9}$$

其中 $c_{ii}=0$，其余 c_{ij} 中有 n 个 1，n 个 -1。令 $C=(c_{ij})$ 为 $2n+1$ 阶方阵，则：

$$\begin{pmatrix} 0 & c_{12} & \cdots & c_{12n+1} \\ c_{21} & 0 & \cdots & c_{22n+1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{2n+11} & c_{2n+12} & \cdots & 0 \end{pmatrix}\begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_{2n+1} \end{pmatrix}=\begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

由于 $(1\ \ 1\cdots 1)^t$ 是上面线性方程组的解，故我们只要证明 $C=(c_{ij})$ 的秩是 $2n$ 即可。

$$\begin{pmatrix} 0 & c_{12} & \cdots & c_{12n+1} \\ c_{21} & 0 & \cdots & c_{22n+1} \\ \vdots & \vdots & \ddots & \vdots \\ c_{2n+11} & c_{2n+12} & \cdots & 0 \end{pmatrix}\xrightarrow{c_1+c_2+\cdots+c_{2n+1}}\begin{pmatrix} 0 & c_{12} & \cdots & c_{12n+1} \\ 0 & 0 & \cdots & c_{22n+1} \\ \vdots & \vdots & \ddots & \vdots \\ 0 & c_{2n+12} & \cdots & 0 \end{pmatrix}$$

由上式知 $C=(c_{ij})$ 的秩不大于 $2n$，我们只需找 $C=(c_{ij})$ 的一个 $2n$ 阶子式不为 0。

$$\begin{pmatrix} 0 & c_{12} & \cdots & c_{12n} \\ c_{21} & 0 & \cdots & c_{22n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{2n1} & c_{2n2} & \cdots & 0 \end{pmatrix}(\mathrm{mod}\,2)=\begin{pmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{pmatrix}$$

$$\det\begin{pmatrix} 0 & 1 & \cdots & 1 \\ 1 & 0 & \cdots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \cdots & 0 \end{pmatrix}=(2n-1)(-1)^{2n-1}=2n-1\not\equiv 0(\mathrm{mod}\,2)\Rightarrow$$

$$\det\begin{pmatrix} 0 & c_{12} & \cdots & c_{12n} \\ c_{21} & 0 & \cdots & c_{22n} \\ \vdots & \vdots & \ddots & \vdots \\ c_{2n1} & c_{2n2} & \cdots & 0 \end{pmatrix}\neq 0,$$

所以 $C=(c_{ij})$ 的秩是 $2n$，则结论成立。

2.2　整系数多项式的整数根问题

例 9　设 $f(x)$ 是 n 次整系数多项式，p 是素数，如果 $f(k), f(k+1),\cdots f(k+p-1)$ 都不被 p 整除，则 $f(x)$ 无整根。

证明: 假设 $f(x)$有整根 α,则 $f(x)=(x-\alpha)f_1(x)$,于是

$$\prod_{i=o}^{p-1} f(k+i)=\prod_{i=0}^{p-1}(k+i-\alpha)f_1(k+i) \qquad (10)$$

$\prod_{i=0}^{p-1}(k+i-\alpha)$是连续 p 个整数之积,故

$\prod_{i=0}^{p-1}(k+i-\alpha)\equiv 0(\mathrm{mod}\ p)$,即

$\prod_{i=0}^{p-1}(k+i-\alpha)f_1(k+i)\equiv 0(\mathrm{mod}\ p)$,再由题设知

$\prod_{i=o}^{p-1} f(k+i)\not\equiv 0(\mathrm{mod}\ p)$ 。

可得(10)式矛盾,所以 $f(x)$无整根。

注记:(ⅰ)例 9 中把素数换成整数 m,其余条件不变,模 p 换成模 m 结论仍然成立。

(ⅱ)当 $p=2$ 时,如果 $f(0)$,$f(1)$都是奇数,则 $f(x)$无整根。

(ⅲ)整系数多项式 $f(x)=\sum_{k=1}^{4n}(-1)^k kx^k+2n+1$ 无整根。

2.3 整系数多项式的不可约性问题

关于整系数多项式的不可约性的判定,我们有 *Eisenstein* 判别法,首先利用模 p(或 p 的方幂)法给出 *Eisenstein* 判别法的一个证明。然后给出此法的应用举例。

命题 4 设 $f(x)=\sum_{i=0}^{n}a_i x^i\in\mathbb{Z}[x]$,$p$ 是素数,如果满足:

(ⅰ)$p\mid a_i, i=0,1,\cdots,n-1$;(ⅱ)$p\nmid a_n$;(ⅲ)$p^2\nmid a_0$

则 $f(x)$在 $Q[x]$中不可约,也在 $Z[x]$中不可约。

证明:假设 $f(x)=g(x)h(x)$,$g(x),h(x)\in Z[x]$,且 $deg(g(x))$,$deg(h(x))<n$ 则 $f(x)=g(x)h(x)\equiv a_n x_n(\mathrm{mod}p)$,由于 $Z/(p)[x]\cong F_p[x]$是 *UFD*(唯一分解环)$\Rightarrow g(x)\equiv ax^k(\mathrm{mod}p)$,$h(x)\equiv bx^{n-k}(\mathrm{mod}p)$,其中 $0<k=deg(g(x))<n$,即 $g(x)$,$h(x)$的常数项都是 p 的倍数,从而 $f(x)=g(x)h(x)$的常数是 p^2 的倍数与题设条件矛盾,所以结论成立。

注记:(ⅰ)命题 4 的证明关键是 $F_p[x]$是唯一分解环,利用分解的唯一性推出多项式系数与条件不符,从而得出结论。

(ⅱ)文献[4]和[5]有类似于命题 4 的结论:

问题 1:设 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+p^2\in Z[x]$,且 $n>2$,p 是素数,如果满足:

①$p^2\mid a_i, i=1,2,\cdots n-1$; ②$p^3\nmid a_1$。则 $f(x)$在 $Q[x]$中不可约。

问题 2:设 p 是素数,且 $n\geq 2$,则 $f(x)=x^n+px+p^2$ 在 $Z[x]$上不可约。

证明:假设 $f(x)=g(x)h(x)$,$g(x),h(x)\in Z[x]$,且 $0<deg(g(x))=s$,$deg(h(x))=t<n$,$f(x)=g(x)h(x)\equiv x^n(\mathrm{mod}p)$,由于 $Z/(p)[x]=F_p[x]$是 *UFD*(唯一分解环),$\Rightarrow g(x)\equiv x^s(\mathrm{mod}p)$,$h(x)\equiv x^t(\mathrm{mod}p)$,可设

$$g(x)=x^s+\sum_{i=0}^{s-1}pb_i x^i,\quad h(x)=x^t+\sum_{j=0}^{t-1}pc_j x^j,$$

若 $s=1$(类似 $t=1$ 地),可知 $f(x)$有整根 p 或 $-p$,这是不可能的。若 $t,s>1$,由于 $p^2=pb_0pc_0$,可得 $b_0c_0=1$,再比较 $f(x)=g(x)h(x)$中的一次项系数知:$p^2(b_1c_0+b_0c_1)=p$,矛盾,故 $f(x)=x^n+px+p^2$ 在 $Z[x]$上不可约。

(ⅲ)用同样处理方法可以证明 Gauss 引理:两个本原多项式之积仍为本原多项式。

例 10 证明 $f(x)=x^4+15x^3+7$ 在 $Z[x]$上不可约。

证明: 由于 $\pm1,\pm7$ 不是 $f(x)=x^4+15x^3+7$ 的有理根,则 $f(x)$没有一次因式。

假设 $f(x)$在 $Z[x]$上可约。$f(x)=g(x)h(x)$,其中 $deg(g(x))=2$,$f(x)=g(x)h(x)\equiv x^2(x^2+x)(\mathrm{mod}7)$,由于 $Z/(7)[x]\cong F_7[x]$是唯一分解环,可设 $g(x)=x^2+7a_1x+7a_0$,$h(x)=x^2+(7b_1+1)x+7b_0\in Z[X]$,比较 $f(x)=g(x)h(x)$中的常数项可得:$7^2a_0b_0=7$,矛盾。故 $f(x)=x^4+15x^3+7$ 在 $Z[x]$上不可约。

例 11 设 n 是任意正整数,则 $f(x)=(x^2+x)2^n+1$ 在 $Z[x]$中不可约。

证明:记 $f(x)=g(h(x))$,其中

$$h(x)=x^2+x,\ g(y)=y2^n+1,$$

$$g(y+1)=(y+1)^{2^n}+1=y^{2^n}+\sum_{k=1}^{2^n-1}\binom{2^n}{k}y^k+2 \qquad (11)$$

取素数 $p=2$,很显然(11)的系数满足命题 4 的 3 个条件,由 *Eisenstein* 判别法知,$g(y+1)$在 $Z[x]$中不可约,从而 $g(x)$在 $Z[x]$中不可约。

首先证明 $f(x)$的任意一个非常数因式的次数不小于 2^n。

假设 $f(x)$可约,即 $f(x)=\varphi(x)f_1(x)$,其中 $\varphi(x)$是 $f(x)$非常数因式,α 是 $\varphi(x)$的一个根,则 $g(h(\alpha))=f(\alpha)=\varphi(\alpha)f_1(\alpha)=0$,记 $s=h(\alpha)$是 $g(x)$的一个根。由于 $s=\alpha^2+\alpha\in Q(\alpha)$,$Q(\alpha)$是 Q 添加 α 形成的域,于是 $Q(s)\subset Q(\alpha)$,因此 $deg(\varphi(x))\geq[Q(\alpha),Q]\geq[Q(s),Q]\geq deg(g(x))=2^n$.($[Q(\alpha),Q]$,$[Q(s),Q]$为域的扩张次数)。

假设 $f(x)=f_1(x)f_2(x)$,$0<deg(f_1(x))$,$deg(f_2(x))<2^{n+1}$,$f(x)=f_1(x)f_2(x)\equiv x^{2^{n+1}}+x^{2^n}+1\equiv(x^2+x+1)^{2^n}(\mathrm{mod}2)$,再由 $Z/(2)[x]\cong F_2[x]$是唯一分解环,及 $f_1(x),f_2(x)$的次数不小于 2^n,$f(x)$的次数是 2^{n+1},可知 $deg(f_1(x))=deg(f_2(x))=2^n$

$\Rightarrow f_1(x)\equiv f_2(x)\equiv(x^2+x+1)^{2^{n-1}}(mod2)$，可设 $f_1(x)=\sum_{i=0}^{2^n} a_i x^i$，$f_2(x)=\sum_{i=0}^{2^n} b_i x^i$，其中系数除 $a_{2^n}, a_{2^{n-1}}, a_0, b_{2^n}, b_{2^{n-1}}, b_0$ 为奇数，其余的都是偶数，由 $f(x)$ 是首 1 的，不失一般性，可设 $a_{2^n}=b_{2^n}=1$，再由 $f(x)$ 无实根及 $f(0)=a_0b_0=1$ 可知 $a_0=b_0=1$，对于 $f_1(x)f_2(x)=f(x)=(x^2+x)2^n+1$ 中的项 $x^{2^n+2^{n-1}}$ 与 $x^{2^{n-1}}$ 项的系数之和模 4 可得

$f(x)$这两项系数之和为 $\binom{2^n}{2^{n-1}}=2\binom{2^n-1}{2^{n-1}-1}\equiv 2(\mathrm{mod}\,2^2)$ (12)

$f_1(x)f_2(x)$这两项系数之和：$\sum_{i+j=2^n+2^{n-1}} a_ib_j+\sum_{i+j=2^{n-1}} a_ib_j$

$$\equiv 2(a_{2^{n-1}}+b_{2^{n-1}})\equiv 0(\mathrm{mod}\,2^2) \quad (13)$$

(12)与(13)式矛盾，因此 $f(x)$ 在 $Z[x]$ 中不可约。

2.4　群论的问题

设 G 是一个有限群，G 的中心为 $Z(G)$，则群类方程 $|G|=|Z(G)|+\sum_i [G:C_G(x_i)]$ (14)

其中在每个多余一个元素的共轭类中取出一个元素 x_i，x_i 的共轭的个数是 $|x_i^G|=[G:C_G(x_i)]$，$[G:C_G(x_i)]$是中心化子$(C_G(x)=\{g\in G \mid gxg^{-1}=x\})$的指数。

如果我们想确定群 G 的某些元素的阶，需要计算 G 的中心(阿贝尔群)所含的个数，而阿贝尔群关于阶或子群有：

命题 5 [6]　如果 G 是有限阿贝尔群，$d\mid|G|$，则 G 含有 d 阶子群。

例 12　(*Cauchy*)如果有限群 G 的阶是素数 p 的倍数，则 G 含有 p 阶元素。

证明：　设 $|G|=mp$，对 $m\geq 1$ 用数学归纳法，当 $m=1$ 时，由拉格朗日定理知 p 阶群中，每一个非单位元的阶都是 p，所以结论成立。

假设对于小于 m 的结论都成立，如果 $x\in G$，则 X 的共轭的个数是 $|x^G|=[G:C_G(x)]$，其中 $C_G(x)=\{g\in G \mid gxg^{-1}=x\}$是 G 的中心化子。如果 $x\notin Z(G)$，则 x 的共轭的个数多于一个，因此 $|C_G(x)|<|G|$。若对某个非中心的 x，有 $p\mid|C_G(x)|$，则由归纳假设知在真子群 $C_G(x)$中有 p 阶元素，从而结论成立。我们假定对一切非中心的 $x\in G$，$p\nmid|C_G(x)|$，因 p 素数且 $|G|=[G:C_G(x)]|C_G(x)|\Rightarrow p\mid[G:C_G(x)]$，我们对(14)式的两边模 p，可得 $|ZG|\equiv 0(\mathrm{mod}p)$，$Z(G)$是阿贝尔群，根据命题 5 知 $Z(G)$(从而 G)中包含 P 阶元素。由数学归纳法原理，所以结论成立。

(ⅰ)如果 P 是素数，$\{1\}\neq G$ 是 P-群，则 $|Z(G)|\equiv 0(\mathrm{mod}p)$。

(ⅱ)如果 P 是素数，则每个阶为 P^2 的群，都是阿贝尔群。

参考文献：

[1]L. J. Mordell, DIOPHANTINE EQUATIONS [M].Academic Press, London and New York, 1969.

[2]柯召，孙琦.数论讲义[M].北京：高教出版社，2001.

[3]R.S. Luthar, American Mathematical Monthly [J].1976,83(7):556.

[4]李克正.抽象代数基础[M].北京：清华大学出版社，2007.

[5] Steven. Roman, Field Theory [M]. (2th edition),Springer-Verlag, Berlin,2006.

[6]Joseph J. Rotman, An Introduction to the Theory of Groups [M].Springer-Verlag, New York,1995.

责任编辑：胡德明

The Method of Mod p and its Application in Elementary Number Theory

Fang Hui, Fang Wei

(Department of Mathematics, Huangshan University, Huangshan 245041, China)

Abstract: Based on mod p (or the power of mod p) method together with properties and findings of prime p, this paper effectively discusses congruence, integral polynomials, integral matrices, and order of groups, etc.

Key words: Prime; Congruence; Mod p method; Quadratic Reciprocity Law

《初等数论》中的模p法及其应用

作者： 方辉， 方炜， Fang Hui， Fang Wei
作者单位： 黄山学院,教学系,安徽,黄山,245041
刊名： 黄山学院学报
英文刊名： JOURNAL OF HUANGSHAN UNIVERSITY
年，卷(期)： 2009，11(3)
引用次数： 0次

相似文献(10条)

1. 学位论文 傅旭丹 素数幂模上的同余式 2007
本文分成三大部分。第一部分，研究整数幂模意义上的同余理论，把Lehmer的一组与(*)形式类似，意义等同的包含欧拉商的同余式推广到任意整数幂模上，并利用这个结论得出一组组合数的公式；还将其另一个有关欧拉数的同余式做到了素数幂模上。 第二部分，考虑Zhao的以下结论S(1，1，1；p)≡-2B<,p>-3(mod p)的自然推广S(α，β，γ，p)(mod p)，其中α，β，γ为任意正整数。得到了S(α，β，γ，p)模p的精确表达式，并且得到几个有关Catalan数的同余式；对于偶数α+β+γ，由于它是p的倍数，所以我们进而考虑了模p<’2>的情况。 第三部分，做了广义二项式系数意义下Babbage，Glaisher和Ljunggren同余式相对应的推广，部分地推广了Andrews的q-模拟的有关结论。

2. 期刊论文 方伟中 关于素数和孪生素数的注记 -天中学刊2001,16(2)
利用Sundaram筛法,给出素数的表示.在此基础上得到了关于素数的判别定理和相应筛法.

3. 期刊论文 张新元 模等差互素的一次同余方程组的求解公式 -科技创新导报2009(10)
本文给出关于一类等差数列中三个相邻互素数的一次同余方程组的求解公式.

4. 期刊论文 王七容.胡付高 组合数的一种同余表示及应用 -山东理工大学学报(自然科学版)2003,17(6)
利用循环群在其子集上的作用,得到组合数的一种同余表示 .讨论了它在数论与代数学中的应用,获得了素数的一个新的判别条件 .

5. 期刊论文 胡付高.苏清华.HU Fu-gao.SU Qing-hua 关于组合数的一些新的同余式 -辽宁工程技术大学学报（自然科学版）2007,26(3)
利用群在集合上的作用的方法,建立组合数的一些新的同余式,这些同余式在证明Sylow定理与Frobenius定理等方面有广泛的应用.借鉴Gallagher的方法,运用循环群在其特定子集组成的集族上的作用,提出了四个关于组合数的同余式的基本引理,在此基础上建立了一些新的同余公式,获得了一些推广的结果,通过这些同余公式给出Frobenius定理的一种巧妙的证明,并且这些同余公式及其推广的结果都可以作为素数的性质定理.

6. 期刊论文 韩璐.肖兆鸾.HAN Lu.XIAO Zhao-luan 一种混合型随机数发生器的研究 -重庆科技学院学报(自然科学版)2008,10(3)
提出了一种混合型随机数算法.该算法将超素数长周期法与乘同余发生器相组合,产生了一种新型的随机数生成方法.经过验证,该算法具有很好的统计性能,并在周期和独立性上都得到了明显的改善,故可作为随机数发生器.

7. 期刊论文 陈小松 分圆多项式系数的上限 -湘潭大学自然科学学报2002,24(3)
利用将多项式分项相除的计算分圆多项式系数的简洁算法,证明了当p1,p2,p3(p 1<p2<p3)为奇素数n=pαllpαp22pα33时,分圆多项式Fn(x)的系数绝对值的一个上限为p1-1.若p2还对模2p1同余于±1,则F n(x)的各系数绝对值不大于(p1+1)/2.

8. 期刊论文 潘琼.田径.PAN Qiong.TIAN Jing 二项式系数幂和序列在模p2下的几个性质 -纯粹数学与应用数学2008,24(1)
利用同余理论和多项式理论研究二项式系数幂和序列在模p2下的同余性质,得到了一些非平凡结果.为进一步研究二项式系数幂和序列的多项式递推公式提供有利的工具.

9. 学位论文 胡海朋 一种新的伪随机数产生方法及其统计性能分析 2007
伪随机数的产生及对伪随机数序列的统计特性进行检验分析是系统仿真技术中的一项基础性研究工作，为特定的目的进行仿真，必须能够提供适当的伪随机数发生器，才能保证仿真的顺利进行。随着计算机计算能力的不断提高，随机数发生器在许多领域有了更加广泛的应用。本文在系统总结已有伪随机数算法的基础上，利用超素数的特殊性质，结合广义位移寄存器产生器的优点，提出了一种新的组合算法—基于超素数法与广义位移寄存器的组合发生器，经过统计检验证明，此组合算法产生的伪随机序列能通过参数检验、均匀性检验、独立性检验等所有检验；根据仿真数据表明此方法产生的伪随机数序列较之其它单独产生算法和其它三种组合法产生的伪随机数序列周期更长、独立性和均匀性更好，是一种更加有效的伪随机数产生算法。

10. 期刊论文 胡付高 Gallagher同余式的表示定理及应用 -北华大学学报(自然科学版)2004,5(1)
研究了组合数的一种同余表示,得到了组合数同余的几个计算公式.