多项式除法解高次同余

◎黄嘉威 （暨南大学信息科技学院数学系，广东 广州 510632）

【摘要】本文研究了高次同余的计算问题，利用公式和递推的方法，推广了多项式除法的结果.

【关键词】同余；费马小定理；组合数；多项式

1. 引言

由费马小定理开始高次同余有了计算方法，欧拉定理把它推广到合数情况，Carmichael 函数更使同余运算更进一步.

本文将透过多项式除法让高次同余运算得到更大的发展.

2. 费马小定理的推广

费马小定理，即当 a 与 p 互素，且 p 为素数时，有 $a^{p-1} \equiv 1 \pmod p$.

这意味着多项式 $x^p - x$ 整除 p [1]，也意味着 $(x^p - x)^m$ 整除 p^m. 展开即:

定理 2.1 $x^{mp} \equiv \sum\limits_{i=1}^{m} (-1)^{i-1} C_m^i x^{mp-(p-1)i} \pmod{p^m}$

用一个例子比较一下这个递推式与欧拉定理 $a^{\varphi(n)} \equiv 1 \pmod n$.

$x^{14} \equiv 2x^8 - x^2 \pmod{7^2}$ $x^{44} \equiv x^2 \pmod{7^2}$

前者能在更小次方的情况下递推，更多的情况下 mp 小于 $(p-1)p^{m-1} + m$.

要是用前者递推高次同余，没能一步过的话会很麻烦，欧拉定理却能一步过.

$x^{1000} \equiv 2x^{994} - x^{988} \equiv 3x^{988} - 2x^{982} \equiv \cdots \pmod{7^2}$ $x^{1000} \equiv x^{34} \pmod{7^2}$

定理 2.2

$$x^{mp+(p-1)n} \equiv \sum_{i=1}^{m} (-1)^{i-1} C_{n+i-1}^{i-1} C_{n+m}^{m-i} x^{mp-(p-1)i} \pmod{p^m}$$

$$x^{14+6n} \equiv C_{n+2}^1 x^8 - C_{n+1}^1 x^2 \pmod{7^2}$$

$$x^{1000} \equiv 166x^{10} - 165x^4 \equiv 19x^{10} - 18x^4 \pmod{7^2}$$

$n = 0$ 时为定理 2.1

假如 $x^{mp+(p-1)k} \equiv \sum\limits_{i=1}^{m} (-1)^{i-1} C_{k+i-1}^{i-1} C_{k+m}^{m-i} x^{mp-(p-1)i} \pmod{p^m}$ 成立，

$$x^{mp+(p-1)(k+1)} \equiv \sum_{i=1}^{m} (-1)^{i-1} C_{k+i-1}^{i-1} C_{k+m}^{m-i} x^{mp-(p-1)i} \equiv C_{k+m}^{m-1} x^{mp} + \sum_{i=2}^{m} (-1)^{i-1} C_{k+i-1}^{i-1} C_{k+m}^{m-i} x^{mp-(p-1)(i-1)}$$

$$\equiv \sum_{i=1}^{m} (-1)^{i-1} C_{k+m}^{m-1} C_m^i x^{mp-(p-1)i} + \sum_{i=1}^{m-1} (-1)^i C_{k+i}^i C_{k+m}^{m-i-1} x^{mp-(p-1)i}$$

$$\equiv (-1)^{i-1} C_{k+m}^{m-1} x^m + \sum_{i=1}^{m-1} (-1)^{i-1}.$$

$$(C_{k+m}^{m-1} C_m^i - C_{k+i}^i C_{k+m}^{m-i-1}) x^{mp-(p-1)i} \pmod{p^m}$$

由于 $(-1)^{m-1} C_{k+1+m-1}^{m-1} C_{k+m}^{m-m} x^{mp-(p-1)m} = (-1)^{i-1} C_{k+m}^{m-1} x^m$，接下来只需证明一条恒等式:

$$C_{k+m}^{m-1} C_m^i - C_{k+i}^i C_{k+m}^{m-i-1} = C_{k+i}^{i-1} C_{k+1+m}^{m-i}.$$

拆开后得到:

$$\frac{(k+m)!\,m!}{(m-1)!\,(k+1)!\,i!\,(m-i)!} - \frac{(k+i)!\,(k+m)!}{i!\,k!\,(m-i-1)!\,(k+i+1)!} = \frac{(k+i)!\,(k+m+1)!}{(i-1)!\,(k+1)!\,(m-i)!\,(k+i+1)!}$$

$$\Leftrightarrow (k+i+1)m - (m-i)(k+1) = i(k+m+1)$$

$$\Leftrightarrow km + im + m - km - m + ik + i = ik + im + i.$$

3. 递推与组合数待定

因为 $P_x^m = m!\,C_x^m$，所以多项式 $P(x,m)$ 必然整除对应的阶乘 $m!$.

定理 3.1 $P_x^m \equiv x(x-1)(x-2)\cdots(x-m+1) \equiv 0 \pmod{m!}$.

考虑 $x^3 \equiv 3x^2 - 2x \pmod 6$，经过两次递推得到 x^4 同余次数小于 3 的多项式:

$$x^4 \equiv 3x^3 - 2x^2 \equiv 3(3x^2 - 2x) - 2x^2 \equiv 7x^2 - 6x^2 \equiv x^2 \pmod 6.$$

定理 3.2 必然存在常系数 c_i 使得 $x^n \equiv \sum\limits_{i=0}^{m-1} c_i x^i \pmod{m!}$. [2]

由于存在着递推关系 $P_x^m \equiv 0 \pmod{m!}$，x^n 必然与次数小于 m 的多项式模 $m!$ 同余.

待定后，当 $x = 0$ 时 x^n 为 0，所以它必然是一个没有常数项的多项式.

例如:

$x^n \equiv c_1x + c_0(\bmod 2!)$

$\begin{cases} c_0 = 0 \\ c_1 + c_0 = 1 \end{cases} \to \begin{cases} c_0 = 0 \\ c_1 = 1 \end{cases} \to x^n \equiv x(\bmod 2!).$

$x^n \equiv c_2x^2 + c_1x + c_0(\bmod 3!).$

$\begin{cases} c_0 = 0 \\ c_2 + c_1 + c_0 = 1 \\ 4c_2 + 2c_1 + c_0 = 2^n \end{cases} \to \begin{cases} c_0 = 0 \\ c_1 = 2 - 2^{n-1} \\ c_2 = 2^{n-1} - 1 \end{cases} \to x^n \equiv (2^{n-1} - 1)x^2 + (2 - 2^{n-1})x(\bmod 3!).$

引理 3.3 $m-2$ **次多项式能待定成含有帕斯卡矩阵的通项**[3]：

$$(C_{x-1}^0 \quad C_{x-1}^1 \quad \cdots \quad C_{x-1}^{m-2})\begin{pmatrix} 1 & 0 & \cdots & 0 \\ -1 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ (-1)^{m-2} & (-1)^{m-1}C_{m-2}^1 & \cdots & 1 \end{pmatrix}\begin{pmatrix} 1^n \\ 2^n \\ \cdots \\ (m-1)^n \end{pmatrix}.$$

推论 3.4 $x^{n+1} \equiv \sum_{i=1}^{m-1} c_ix^i \equiv x\sum_{i=0}^{m-2} d_iC_{x-1}^i(\bmod m!)n \geqslant m-1$

$$x^{n+1} \equiv x(C_{x-1}^0 \quad C_{x-1}^1 \quad \ldots \quad C_{x-1}^{m-2})\begin{pmatrix} 1 & 0 & \cdots & 0 \\ -1 & 1 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots \\ (-1)^{m-2} & (-1)^{m-1}C_{m-2}^1 & \cdots & 1 \end{pmatrix}\begin{pmatrix} 1^n \\ 2^n \\ \ldots \\ (m-1)^n \end{pmatrix}.$$

例如：

$x^{n+1} \equiv x(C_{x-1}^0)(1)(1^n) \equiv x(\bmod 2).$

$x^{n+1} \equiv x(C_{x-1}^0 \quad C_{x-1}^1)\begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}\begin{pmatrix} 1^n \\ 2^n \end{pmatrix} \equiv x(1 \quad x-1)\begin{pmatrix} 1 \\ 2^n - 1 \end{pmatrix} \equiv x[1 + (2^n - 1)(x-1)] \equiv (2^n - 1)x^2 + (2 - 2^n)x(\bmod 6).$

代入 $n = 2, 3$ **可得** $x^3 \equiv 3x^2 - 2x(\bmod 6), x^4 \equiv 7x^2 - 6x \equiv x^2(\bmod 6).$

【参考文献】

[1] 潘承洞. 数论基础[M]. 北京：高等教育出版，2012.

[2] 韩士安，林磊. 近世代数[M]. 北京：科学出版社，2009.

[3] 黄婷，车茂林，彭杰，张莉. 自然数幂和通项公式证明的新方法[J]. 内江师范学院学报，2011.8.

（上接103页）

二、可化为常系数线性非齐方程的方程——欧拉方程的解法

欧拉方程的解法一般步骤是：先写出欧拉方程的特征方程，并求出特征根；再求出其基本组解，最后写出原方程的通解. 如下例：

例 求解方程 $x^2y'' - 3xy' - 5y = x^2\ln x.$

解 这是一个欧拉方程，令 $t = \ln x, x = e^t$，则

$y' = \frac{dy}{dt} \cdot \frac{dt}{dx} = \frac{1}{x}y_t'$，

$y'' = \frac{1}{x^2}y_t' + \frac{1}{x}y_t'' \cdot \frac{dt}{dx} = \frac{1}{x^2}(y_t'' - y_t')$，

代入原方程，得

$y_t'' - 4y_t' - 5y = te^{2t}.$ ①

和①对应的齐次方程为：

$y_t'' - 4y_t' - 5y = 0.$ ②

②的特征方程为 $r^2 - 4r - 5 = 0$，特征根为 $r_1 = 5, r_2 = -1$，

则②的通解为 $Y = C_1e^{5t} + C_2e^{-t}.$

设①的特解为 $y^* = (at + b)e^{2t}$，则

$(y^*)' = e^{2t}(2at + a + 2b)$，

$(y^*)'' = e^{2t}(4at + 4a + 4b)$，

将 $y^*, (y^*)', (y^*)''$ 代入原方程比较系数，

得 $-9at - 9b = t.$

$\therefore a = -\frac{1}{9}, b = 0, y^* = -\frac{1}{9}te^{2t}.$

得①的通解为 $y = C_1e^{5t} + C_2e^{-t} - \frac{1}{9}te^{2t}$. 故原方程的通解为 $y = C_1x^5 + \frac{C_2}{x} - \frac{1}{9}x^2\ln x.$

三、总　结

高阶微分方程的问题一般比较复杂，在具体求解时应根据微分方程的特点，具体问题具体对待，将微分方程化为易于求解的形式，只有这样才能达到简化易解的程度.

【参考文献】

[1] George F. simmons, Steven G. krantz. Differential Equations: Theory, Technique, and Practice [M]. Beijing: tsinghua university press, 2009.

[2] 时宝，黄朝炎. 微分方程基础及其应用[M]. 北京：科学出版社，2007.

[3] 李瑞遐. 应用微分方程[M]. 上海：华东理工大学出版社，2005.