第 12 卷 第 5 期　　电 子 科 学 学 刊　　Vol. 12, No. 5
1990 年 9 月　　JOURNAL OF ELECTRONICS　　Sept., 1990

$Z/(m)$ 上线性递归序列的有关问题*

李 献 刚
(郑州信息工程学院应用数学系，郑州)

摘要　本文主要讨论了剩余类环 $Z/(m)$ 上线性递归序列的周期，计数，分布以及与其相关联的 $Z/(m)[x]$ 中多项式的有关问题.

关键词　线性递归序列；源(拟)多项式；源(拟) m-序列；周期

一、引　言

线性递归序列在信道编码和流密码体制的设计与分析中有着广泛的应用[1,2]. 有限域上线性递归序列的研究已较成熟[3,4]，而有限 Z-模上线性递归序列的分析问题又可转化为模素数方幂的剩余类环 $Z/(p^e)$ 上的分析问题去研究[5]. 对剩余类环 $Z/(m)$ 上递归序列的研究和应用已引起了人们越来越多的重视[6-11]. 本文将深入讨论这类序列的周期，计数，分布问题以及与其有关的其它课题. 由于篇幅所限，我们仅给出所用到的引理以及有关结论，详细证明可参见文献[12]和[13].

设 m、n 均为正整数，$Z/(m)$ 是模 m 的剩余类环，$a_0, a_1, \cdots, a_{n-1}$ 是 $Z/(m)$ 中的元素，且满足 $(a_0, m) = 1$，则由下式确定的 $Z/(m)$ 上的序列

$$u_{t+n} = a_{n-1}u_{t+n-1} + \cdots + a_1u_{t+1} + a_0u_0 \in Z/(m),\ t \geqslant 0 \tag{1}$$

称为 $Z/(m)$ 上的 n 级线性递归序列，记为 $\tilde{u} = (u_t)$，$u_0 = (u_0, u_1, \cdots, u_{n-1})$ 称为 $\tilde{u}$ 的初态，而多项式

$$f(x) = x^n + a'_{n-1}x^{n-1} + \cdots + a'_1x + a'_0 \in Z/(m)[x] \tag{2}$$

称为 $\tilde{u}$ 的一个生成多项式. 其中 $a'_i = -a_i$，$0 \leqslant i \leqslant n-1$. 同样可类似有限域中线性递归序列的概念定义 $Z/(m)$ 上序列的周期、极小多项式以及 $Z/(m)[x]$ 中多项式周期的概念. 精确定义可参见文献[3]. 为方便起见，仍引用文献[12]中的记号，且总是设 $m = p^e$，n 为递归序列的阶数，$n \geqslant 2$，其中 $p > 2$ 为素数，$e \geqslant 1$. 令 $\Omega(Z/(p^e)) = \{\tilde{u} = (u_t) \mid u_t \in Z/(p^e),\ t \geqslant 0\}$；$P_n[Z/(p^e), x] = \{f(x) \in Z/(p^e)[x] \mid f(x)$ 首一，$\deg f(x) = n$，且 $(f(0), p) = 1\}$；$\Omega(Z/(p^e), f) = \{\tilde{u} = (u_t) \mid \tilde{u}$ 以 $f(x)$ 为一生成多项式$\}$. 用 A_f 记 $\tilde{u}$ 的状态转移矩阵，即

$$A_f = \begin{bmatrix} 0 & 0 & \cdots & 0 & -a'_0 \\ 1 & 0 & \cdots & 0 & -a'_1 \\ 0 & 1 & \cdots & 0 & -a'_2 \\ \cdots & & \cdots & & \cdots \\ 0 & 0 & \cdots & 1 & -a'_{n-1} \end{bmatrix} = \begin{bmatrix} 0 & 0 & \cdots & 0 & a_0 \\ 1 & 0 & \cdots & 0 & a_1 \\ 0 & 1 & \cdots & 0 & a_2 \\ \cdots & & \cdots & & \cdots \\ 0 & 0 & \cdots & 1 & a_{n-1} \end{bmatrix} \tag{3}$$

* 1989 年 6 月 10 日收到，1989 年 12 月修改定稿.

若 $f(x)\in P_n[Z/(p^e),x]$，$\tilde{u}\in Q(Z/(p^e),f)$，$u_t=(u_t,u_{t+1},\cdots,u_{t+n-1})\in Z/(p^e)\otimes\cdots\otimes Z/(p^e)$，$A_f\in M_n(Z/(p^e))(Z/(p^e))$上的 n 阶矩阵环)，则 $1\leqslant r\leqslant e$ 时，总可在同态意义下将它们看作 $P_n[Z/(p^r),x]$，$Q(Z/(p^r),f)$，$Z/(p^r)\otimes\cdots\otimes Z/(p^r)$ 或 $M_n(Z/(p^r))$ 中的元素，分别记为 $f(x)(\mathrm{mod}p^r)$，$\tilde{u}(\mathrm{mod}p^r)$，$u_t(\mathrm{mod}p^r)$ 和 $A_f(\mathrm{mod}p^r)$. 显然，$A_f(\mathrm{mod}p^r)$ 是可逆的. 而 0 总是代表某一代数系统中的零元. 其它一些常用记号为：$\pi_{p^r}(\tilde{u})=\min\{s>0\mid u_{t+s}=u_t(\mathrm{mod}p^r),\ t\geqslant 0\}$，$\pi_{p^r}(f)=\min\{k>0\mid f(x)\mid x^k-1(\mathrm{mod}p^r)\}$，$\mathrm{ord}_{p^r}(A_f)=A_f(\mathrm{mod}p^r)$ 在 $M_n(Z/(p^r))$ 中的阶，$m_{p^r}(\tilde{u},x)=\tilde{u}(\mathrm{mod}p^r)$ 在 $Z/(p^r)[x]$ 中的极小多项式.

二、线性递归序列的周期

下面在未加说明的情况下，总是设 $f(x)\in P_n[Z/(p^e),x]$，$\tilde{u}\in Q(Z/(p^e),f)$，且令

$$C_{\tilde{u}}=(u_0,u_1,\cdots,u_{n-1})^{tr}=\begin{bmatrix}u_0, & u_1, & \cdots & u_{n-1}\\ u_1, & u_2, & \cdots & u_n\\ \cdots & \cdots & \cdots & \cdots\\ u_{n-1} & u_n, & \cdots & u_{2n-1}\end{bmatrix}\tag{4}$$

用 $|C_{\tilde{u}}|$ 表示 $C_{\tilde{u}}$ 的行列式值.

命题 1　若 $|C_{\tilde{u}}|\not\equiv 0(\mathrm{mod}p)$，即 u_0，u_1，$\cdots$，u_{n-1} 对于 $Z/(p)$ 线性无关，则 $\pi_{p^e}(\tilde{u})=\mathrm{ord}_{p^e}(A_f)$.

令 $d_0=(0,0,\cdots,0,1)\in Z/(p^e)\otimes\cdots\otimes Z/(p^e)$，记 $\tilde{d}\in Q(Z/(p^e),f)$ 是以 d_0 为初态的序列，由于

$$C_{\tilde{d}}=\begin{bmatrix}0 & 0 & \cdots & 0 & 1\\ 0 & 0 & \cdots & 1 & *\\ \cdots & \cdots & \cdots & \cdots & \cdots\\ 0 & 1 & \cdots & * & *\\ 1 & * & \cdots & * & *\end{bmatrix}(\mathrm{mod}p^e)$$

显然 $|C_{\tilde{d}}|=1(\mathrm{mod}p)$. 由命题 1 可得

定理 1　$\pi_{p^e}(\tilde{d})=\mathrm{ord}_{p^e}(A_f)$，即 $\tilde{d}$ 总能达到 $A_f(\mathrm{mod}p^e)$ 的阶数.

命题 2　若 $u_0(\mathrm{mod}p)\not\equiv 0$，且 $f(x)(\mathrm{mod}p)=m_p(\tilde{u},x)$，则 $\pi_{p^e}(\tilde{u})=\mathrm{ord}_{p^e}(A_f)$.

定理 2　若存在 $r(0\leqslant r\leqslant e-1)$，使 $u_0(\mathrm{mod}p^r)=0$，$u_0(\mathrm{mod}p^{r+1})\not\equiv 0$，且 $f(x)(\mathrm{mod}p^{r+1})=m_{p^{r+1}}(\tilde{u},x)$，则 $\pi_{p^e}(\tilde{u})=\mathrm{ord}_{p^{e-r}}(A_f)$.

定理 3　任给 $f(x)\in P_n[Z/(p^e),x]$ 有 $\pi_{p^e}(f)=\mathrm{ord}_{p^e}(A_f)$.

由上述定理可得 $\tilde{u}\in Q(Z/(p^e),f)$ 的周期性质如下：

定理 4　若整数 r，$r_0(0\leqslant r$，$r_0\leqslant e-1)$ 满足：(1) $\pi_{p^e}(f)=p^r\cdot\pi_p(f)$；(2) $u_0(\mathrm{mod}p^{r_0})=0$，但 $u_0(\mathrm{mod}p^{r_0+1})\not\equiv 0$；(3) $f(x)(\mathrm{mod}p^{r_0+1})=m_{p^{r_0+1}}(\tilde{u},x)$，则 $\pi_{p^e}(\tilde{u})$ 满足：

$$\pi_{p^e}(u)=\begin{cases}\pi_p(f), & \text{若 } 0\leqslant r\leqslant r_0\\ p^{r-r_0}\pi_p(f), & \text{若 } 0\leqslant r_0<r\end{cases}$$

定理 5　若 $f(x)(\mathrm{mod}p)$ 不可约，且 $\pi_{p^e}(f)=p^r\cdot\pi_p(f)$，$(0\leqslant r\leqslant e-1)$，

$r_0(0 \leqslant r_0 \leqslant e-1)$ 满足 $u_0(\mathrm{mod}p^{r_0}) = 0$, $u_0(\mathrm{mod}p^{r_0+1}) \neq 0$, 则

$$\pi_{p^e}(\tilde{u}) = \begin{cases} \pi_p(f), & \text{若 } 0 \leqslant r \leqslant r_0 \\ p^{r-r_0}\pi_p(f), & \text{若 } 0 \leqslant r_0 < r \end{cases}$$

我们知道 $\pi_p(f) \leqslant \pi_{p^e}(f) \leqslant p^{e-1} \cdot \pi_p(f)$ [12]. 若 $\pi_{p^e}(f) = \pi_p(f)$, 则称 $f(x) \in Z/(p^e)[x]$ 为一源(周期)多项式. 当 $\pi_{p^e}(f) = p^{e-1} \cdot \pi_p(f)$ 时, 称 $f(x)$ 为拟多项式. 当 $f(x)(\mathrm{mod}p)$ 又是不可约(或本原)时,又有源(拟)不可约(或本原)多项式的概念.

推论 1 若 $f(x)$ 是拟不可约多项式,则 $\pi_{p^e}(\tilde{u}) = p^{e-r-1} \cdot \pi_p(f)$ $(0 \leqslant r \leqslant e-1)$, 当且仅当 $u_0(\mathrm{mod}_{p^r}) = 0$, 但 $u_0(\mathrm{mod}p^{r+1}) \neq 0$.

同样, 我们也知道 $\pi_p(\tilde{u}) \leqslant \pi_{p^e}(\tilde{u}) \leqslant p^{e-1} \cdot \pi_p(\tilde{u})$ [11]. 若 $\pi_{p^e}(\tilde{u}) = \pi_p(\tilde{u})$, 则常称 $\tilde{u}$ 为源(周期)序列,特别当 $\pi_{p^e}(\tilde{u}) = p^n - 1 = \pi_p(\tilde{u})$ 时, 称 $\tilde{u}$ 为源 m-序列. 而当 $\tilde{u}$ 为 $\Omega(Z/(p^e), f)$ 中最长周期序列时, 称 $\tilde{u}$ 为拟序列, 若 $\tilde{u}$ 又满足 $\pi_{p^e}(\tilde{u}) = p^{e-1} \cdot (p^n - 1)$, 则称 $\tilde{u}$ 为拟 m-序列.

推论 2 $\Omega(Z/(p^e), f)$ 中序列均为源序列的充要条件是 $f(x) \in P_n[Z/(p^e), x]$ 为一个源多项式.

推论 3 若 $\pi_{p^e}(f) = p^r \cdot \pi_p(f)$, 则 $\tilde{u}$ 为源 m-序列,当且仅当 $f(x)(\mathrm{mod}p)$ 为本原,且 $u_0(\mathrm{mod}p^r) = 0$.

推论 4 $\tilde{u}$ 为 $Z/(p^e)$ 上的 n 阶拟 m-序列,当且仅当 $f(x)$ 为拟本原多项式, 且 $u_0(\mathrm{mod}p) \neq 0$.

三、多项式的周期与计数

对于 $f(x) \in P_n[Z/(p^e), x]$ 的周期,首先有如下一些结论.

定理 6 若 $f(x) \in P_n[Z/(p^e), x]$, 则 $\pi_{p^e}(f) = p^r \cdot \pi_p(f)$, $(0 \leqslant r \leqslant e-1)$, 当且仅当 $f(x)$ 满足如下条件之一: (1) $\pi_{p^{e-r}}(f) = \pi_p(f)$, 且 $\pi_{p^{e-r+1}}(f) = p \cdot \pi_p(f)$; (2) 存在 $u(x)$, $v(x) \in Z[x]$, 且 $v(x)(\mathrm{mod}p) \neq 0$, 使

$$x^{\pi_p(f)} - 1 = f(x)u(x) + p^{e-r} \cdot v(x) \ (\mathrm{mod}\ p^{e-r+1})$$

推论 5 若 $\pi_{p^e}(f) = p^r \cdot \pi_p(f)$, $(0 \leqslant r \leqslant e-1)$, 则

$$\pi_{p^k}(f) = \begin{cases} \pi_p(f), & \text{若 } 0 < k \leqslant e-r \\ p^{k+r-e} \cdot \pi_p(f), & \text{若 } e-r < k \leqslant e \end{cases}$$

推论 6 若 $f(x)(\mathrm{mod}p)$ 不可约, 则 $f(x)$ 是 $Z/(p^e)$ 上的拟不可约多项式, 当且仅当 $\pi_{p^2}(f) = p \cdot \pi_p(f)$.

推论 7 $f(x)$ 是 $Z/(p^e)$ 上的拟本原多项式,当且仅当 $\pi_{p^2}(f) = p(p^n - 1)$, 即 $f(x)(\mathrm{mod}p^2)$ 为拟本原的.

关于 $f(x)$ 的进一步结果是以定理 7 为基础, 它实际上是 p-adic 整数环 Z_p 上的 Hensel's 引理[14]在 $Z/(p^e)[x]$ 上的一种表示形式, 由于它的证明实际上给出了一种求源多项式的算法,因此将以附录形式给出它的证明.

定理 7 (Hensel's 引理) 设 $F(x) \in Z/(p^e)[x]$ 是首一多项式, $f_0(x)$、$g_0(x) \in Z/(p)[x]$ 也为首一多项式,满足 $(f_0(x), g_0(x)) = 1$, 且有 $F(x) = f_0(x) \cdot g_0(x)$ $(\mathrm{mod}p)$,

则存在唯一的一个多项式序列 $f_1(x)、g_1(x)、f_2(x)、g_2(x)、\cdots、f_{e-1}(x)、g_{e-1}(x)$，使得任给 $k(0\leqslant k\leqslant e-1)$，就有：(1) $f_k(x)、g_k(x)\in Z/(p^{k+1})[x]$；(2) $\deg f_k(x)=\deg f_0(x)$，$\deg g_k(x)=\deg g_0(x)$；(3) $f_k(x)\equiv f_{k-1}(x)\pmod{p^k}$，$(f_{-1}(x)\triangleq 0)$，$g_k(x)\equiv g_{k-1}(x)\pmod{p^k}$，$(g_{-1}(x)\triangleq 0)$. 且 $F(x)\equiv f_k(x)g_k(x)\pmod{p^{k+1}}$.

推论 8　设 $F(x)\in Z/(p^e)[x]$ 是首一多项式，且 $F(x)\pmod p$ 无重根，若 $f_0(x)\in Z/(p)[x]$ 也是首一多项式，且 $f_0(x)\mid F(x)\pmod p$，则存在唯一的一个首一多项式 $f_{e-1}(x)\in Z/(p^e)[x]$，满足：(1) $f_{e-1}(x)\equiv f_0(x)\pmod p$，且 $\deg f_{e-1}(x)=\deg f_0(x)$；(2) $f_{e-1}(x)\mid F(x)\pmod{p^e}$.

为讨论 $P_n[Z/(p^e),x]$ 中多项式的周期问题，首先定义如下等价关系，若 $f(x)$，$g(x)\in P_n[Z/(p^e),x]$，则 $f(x)\sim g(x)\Leftrightarrow f(x)\equiv g(x)\pmod p$，用 $[f(x)]_{p^e}$ 表示 $f(x)$ 在 $P_n[Z/(p^e),x]$ 中决定的等价类. 显然，$g(x)\in[f(x)]_{p^e}\Leftrightarrow$ 存在 $v(x)\in Z/(p^{e-1})[x]$，使 $g(x)\equiv f(x)+pv(x)\pmod{p^e}$. 并且任给 $g(x)\in[f(x)]_{p^e}$，就有

$$\pi_p(g)=\pi_p(f)$$

命题 3　若 $f(x)\in P_n[Z/(p^e),x]$，且 $f(x)\pmod p$ 无重根，则 $[f(x)]_{p^e}$ 中含有唯一的一个源多项式，即存在唯一的一个多项式，记为 $f_{e-1}(x)\in[f(x)]_{p^e}$，满足

$$\pi_{p^e}(f_{e-1})=\pi_p(f_{e-1})=\pi_p(f)$$

由命题 3，我们可称 $f_{e-1}(x)$ 为 $[f(x)]_{p^e}$ 或 $f(x)$ 的源多项式，它是 $[f(x)]_{p^e}$ 中的最小周期多项式，且以后总设 $f(x)\pmod p$ 无重根. 文献[13]中讨论了部分有重根的情况.

若令

$$f_k(x)\equiv f_{e-1}(x)\pmod{p^{k+1}},\ (0\leqslant k\leqslant e-1) \tag{5}$$

则显然 $f_k(x)\pmod{p^{k+1}}$ 是 $P_n[Z/(p^{k+1}),x]$ 的一个源多项式. 令

$$\begin{aligned} f_k^* = \{&f_{e-1}(x)+p^k u(x)\mid u(x)\in Z/(p^{e-k})[x]\\ &\deg u(x)<n,\ \text{且}\ u(x)\pmod p\neq 0\} \end{aligned} \tag{6}$$

$$f_0^*=\{f_{e-1}(x)\}$$

其中 $1\leqslant k\leqslant e-1$，则 $f_k^*\subset[f_{e-1}(x)]_{p^e}$. 且有

引理 1　设 $f(x)\in P_n[Z/(p^e),x]$，且 $f_{e-1}(x)$ 为 $[f(x)]_{p^e}$ 的源多项式，$f_k(x)$、$f_k^*(0\leqslant k\leqslant e-1)$ 如上所述，则有：(1) $f_k^*=\{f_k(x)+p^k\cdot u(x)\mid u(x)\in Z/(p^{e-k})[x]$，$\deg u(x)<n$，且 $u(x)\pmod p\neq 0\}$；(2) $[f(x)]_{p^e}=[f_{e-1}(x)]_{p^e}=\bigcup\limits_{0\leqslant k\leqslant e-1}f_k^*$；(3) $f_k^*\cap f_{k'}^*=\phi\Leftrightarrow k\neq k'$，$(0\leqslant k,\ k'\leqslant e-1)$；(4) 若 $g(x)\equiv f_{e-1}(x)+p^k\cdot u(x)\in f_k^*$，且 $h(x)\equiv f_{e-1}(x)+p^k\cdot v(x)\in f_k^*$，则 $g(x)\equiv h(x)\pmod{p^{k+1}}\Leftrightarrow u(x)\equiv v(x)\pmod p$.

引理 2　若 $f(x)\in[f_{e-1}(x)]_{p^e}$，则 $f(x)\in f_k^*$，$(0\leqslant k\leqslant e-1)$，当且仅当：(1) 当 $k=0$ 时，$\pi_{p^e}(f)=\pi_p(f)$；(2) 当 $k>0$ 时，$\pi_{p^k}(f)=\pi_p(f)$，且 $\pi_{p^{k+1}}(f)=p\pi_p(f)$.

由引理 1 和引理 2，可得关于 $f(x)$ 周期的如下一些结论.

定理 8　若 $f(x)\in P_n[Z/(p^e),x]$，$f_{e-1}(x)$ 为 $[f(x)]_{p^e}$ 的源多项式，$f_k(x)$、f_k^*

$(0 \leqslant k \leqslant e-1)$ 如(5)式和(6)式所定义,则 $\pi_p{}^e(f) = p^r \cdot \pi_p(f)$, $(0 \leqslant r \leqslant e-1)$. 当且仅当 $f(x)$ 满足如下条件之一: (1) $f(x) \in \underline{f}_{e-r}^*$ (记 $\underline{f}_e^* = \underline{f}_0^*$); (2) 存在 $u(x) \in Z/(p^r)[x]$, 且 $u(x) \pmod p \neq 0$, 使 $f(x) = f_{e-1}(x) + p^{e-r} \cdot u(x) \pmod{p^e}$; (3) $f(x) = f_{e-1}(x) \pmod{p^{e-r}}$, 但 $f(x) \neq f_{e-1}(x) \pmod{p^{e-r+1}}$.

推论 9 若 $f_{e-1}(x) \in P_n[Z/(p^e), x]$ 为一源多项式,而 $f(x) \in [f_{e-1}(x)]_{p^e}$, 则: (1) $f(x)$ 为拟多项式, 即 $\pi_p{}^e(f) = p^{e-1} \cdot \pi_p(f)$, 当且仅当 $f(x) \in \underline{f}_1^*$, 即 $f(x) \fallingdotseq f_{e-1}(x) \pmod{p^2}$; (2) $f(x)$ 为拟不可约多项式, 当且仅当 $f(x) \pmod p$ 不可约, 且 $f(x) \fallingdotseq f_{e-1}(x) \pmod{p^2}$; (3). $f(x)$ 为拟本原多项式, 当且仅当 $f_{e-1}(x) \pmod p$ 本原, 且 $f(x) \fallingdotseq f_{e-1}(x) \pmod{p^2}$, 这时 $f(x)$ 为最大周期多项式.

由上述的一些结论可知,我们的主要问题转化为如何求出 $f(x) \in P_n[Z/(p^e), x]$ 的源多项式 $f_{e-1}(x)$. 求有限域上多项式的周期已有许多方法,因此, 由附录中定理 7 的构造性证明方法,我们很容易给出求 $f_{e-1}(x)$ 的算法,并由此确定出 $\pi_p{}^e(f)$ 的值. 我们假设 $\pi_p(f)$ 的值已经求出.

算法(求源多项式和 $f(x)$ 的周期) 输入为多项式 $f(x) \in P_n[Z/(p^e), x]$ 和整数 $N = \pi_p(f)$. 输出为 $f(x)$ 的源多项式 $f_{e-1}(x)$ 和周期 $\pi_p{}^e(f)$. (1) 计算 $f_0(x) \in Z/(p)[x]$, 使 $f_0(x) = f(x) \pmod p$; (2) 用 $f_0(x)$ 除以 $x^N - 1$, 得 $g_0(x)$, 使 $x^N - 1 = f_0(x) \cdot g_0(x) \pmod p$; (3) 由附录中定理 7 的构造性证明方法依次求出 $f_k(x) \pmod{p^{k+1}}$, $(0 \leqslant k \leqslant e-1)$; (4) 求出满足 $f(x) = f_{e-1}(x) \pmod{p^k}$ 和 $f(x) \fallingdotseq f_{e-1}(x) \pmod{p^{k+1}}$ 的正整数 k; (5) 输出 $f_{e-1}(x)$ 和 $\pi_p{}^e(f) = p^{e-k} \cdot \pi_p(f)$.

上述算法实际上仅依赖于 $Z[x]$ 中的 Eulidean 除法, 因此并不困难. 第 1 行到第 3 行可使我们求得 $f(x)$ 的源多项式. 若我们仅希望求出 $f(x)$ 的周期, 则第 3 行的步骤只需找到 k, 使 $f(x) = f_{k-1}(x) \pmod{p^k}$ 和 $f(x) \neq f_k(x) \pmod{p^{k+1}}$ 即可得 $\pi_p{}^e(f) = p^{e-k} \cdot \pi_p(f)$. 这样,就基本解决了 $f(x) \pmod p$ 无重根的多项式的周期问题.

由定理 8 我们还可得到一些关于给定周期的 $P_n[Z/(p^e), x]$ 中多项式的计数问题.

命题 4 若 $f(x) \in P_n[Z/(p^e), x]$, 则在 $[f(x)]_{p^e}$ 中共有 $p^{rn} \cdot (1 - p^{-n})$ 个多项式满足 $\pi_p{}^e(g) = p^r \cdot \pi_p(g) = p^r \cdot \pi_p(f)$, $(0 \leqslant r \leqslant e-1)$, 其中 $g(x) \in [f(x)]_{p^e}$.

命题 5 在 $P_n[Z/(p^e), x]$ 中源不可约多项式的个数为

$$\left(\frac{1}{n}\right) \sum_{d \mid n} \mu(n/d) \cdot p^d = \left(\frac{1}{n}\right) \sum_{d \mid n} \mu(d) \cdot p^{n/d}$$

源本原多项式的个数为 $\varphi(p^n - 1)/n$.

命题 6 关于 $P_n[Z/(p^e), x]$ 中的拟多项式有如下结论: (1) 任给 $f(x) \in P_n[Z/(p^e), x]$, $[f(x)]_{p^e}$ 中共有 $p^{(e-1)n} \cdot (1 - 1/p^n)$ 个拟多项式; (2) $P_n[Z/(p^e), x]$ 中拟不可约多项式的个数为 $p^{(e-1)n} \cdot (1 - 1/p^n) \cdot (1/n) \cdot \sum_{d \mid n} \mu(n/d) \cdot p^d$; (3) $P_n[Z/(p^e), x]$ 中拟本原多项式的个数为 $p^{(e-1)n} \cdot (1 - 1/p^n) \cdot \varphi(p^n - 1)/n$.

作为应用,我们可重新描述推论 2 和推论 4 关于序列周期的结论.

定理 9 若 $f(x) \in p_n[Z/(P^e), x]$, $f_{e-1}(x)$ 为 $f(x)$ 的源多项式, $\tilde{u} \in \Omega(Z/(p^e), f)$, 则 (1) 若 $f_{e-1}(x) \pmod p$ 不可约,则 $\pi_p{}^e(\tilde{u}) = p^{e-1} \cdot \pi_p(\tilde{u})$, 当且仅当 $f(x) \fallingdotseq f_{e-1}(x)$

$(\mathrm{mod}p^2)$，且 $u_0(\mathrm{mod}p)\neq 0$；(2). $\tilde{u}$ 为拟 m-序列，当且仅当 $f(x)\neq f_{e-1}(x)(\mathrm{mod}p^2)$，$f_{e-1}(x)$ $(\mathrm{mod}p)$ 为本原的，且 $u_0(\mathrm{mod}p)\neq 0$.

四、线性递归序列的圈数

用 $N_f(Z/(p^e))$ 记 $\mathcal{Q}(Z/(p^e),f)$ 中非平移等价的序列的个数，文献[11]中曾证明了如下定理.

定理 10　若 $f(x)\in P_n[Z/(p^e),x]$，则 (1) $N_f(Z/(p^e))\geqslant e+1$；

(2) $N_f(Z/(p^e))\geqslant 2^e$；　(3) $N_f(Z/(p^e))\geqslant\dfrac{(p^{(n-1)e}-1)(p^n-1)}{(p^{(n-1)}-1)\cdot\pi_p(f)}+1$

关于 $N_f(Z/(p^e))$，我们还有如下一些进一步的结论.

定理 11　若 $f(x)\in P_n[Z/(p^e),x]$，且 $f(x)(\mathrm{mod}p)$ 不可约，则

(1)　$\dfrac{(p^{(n-1)e}-1)(p^n-1)}{(p^{(n-1)}-1)\cdot\pi_p(f)}+1\leqslant N_f(Z/(p^e))\leqslant(p^{ne}-1)/\pi_p(f)+1$

(2) 若 $\pi_{p^e}(f)=p^r\cdot\pi_p(f)$，　$(0\leqslant r\leqslant e-1)$，则有

$$N_f(Z/(p^e))=\left(\frac{p^{(e-r)n}-1}{\pi_p(f)}\right)+\left(\frac{p^{en-r}-p^{(e-r)n}}{\pi_p(f)}\right)\left(1-\frac{1}{p^n}\right)\left(1-\frac{1}{p^{n-1}}\right)^{-1}+1$$

推论 10　若 $f(x)\in P_n[Z/(p^e),x]$ 为源不可约多项式，则

$$N_f(Z/(p^e))=(p^{en}-1)/\pi_p(f)+1$$

推论 11　若 $f(x)\in P_n[Z/(p^e),x]$ 为拟不可约多项式，则

$$N_f(Z/(p^e))=[(p^{e(n-1)}-1)(p^n-1)]/[(p^{n-1}-1)\pi_p(f)]+1$$

对于源 m-序列有如下定理.

定理 12　若 $f(x)\in P_n[Z/(p^e),x]$，$f(x)$ $(\mathrm{mod}p)$ 本原，且 $\pi_p(f)=p^r\cdot(p^n-1)$，$(0\leqslant r\leqslant e-1)$，则在 $\mathcal{Q}(Z/(p^e),f)$ 中共有 $(p^{(e-r)n}-1)/(p^n-1)$ 个非平移等价的源 m-序列. 而 $\mathcal{Q}(Z/(p^e))$ 中所有非平移等价的 n 阶源 m-序列的个数为

$$[e\cdot p^{(e+1)n}-(e+1)\cdot p^{en}+1][p^n\cdot(p^n-1)]^{-1}\cdot\varphi(p^n-1)/n$$

关于拟 m-序列我们有

定理 13　若 $f(x)\in P_n[Z/(p^e),x]$ 为拟本原多项式，则 $N_f(Z/(p^e))=(p^{e(n-1)}-1)/(p^{(n-1)}-1)+1$，且 $\mathcal{Q}(Z/(p^e),f)$ 中非平移等价的拟 m 序列的个数为 $p^{(n-1)(e-1)}$. 进一步 $\mathcal{Q}(Z/(p^e))$ 中共有 $p^{(2n-1)(e-1)}\cdot(1-p^{-n})\varphi(p^n-1)/n$ 个非平移等价的 n 级拟 m-序列.

五、线性递归序列的分布

用 $Z_{p^e}(b:\tilde{u})$ 记 $b\in Z/(p^e)$ 在 $\tilde{u}$ 的一个周期段内出现的次数，为讨论 $Z_{p^e}(b:\tilde{u})$ 的有关性质，类似于有限域上加性特征标的概念，我们引入 $Z/(p^e)$ 上特征标的概念，设 U

为复数域中模为 1 的复数组成的乘法子群，$Z/(p^e)$ 上的一个特征标是一个从 $(Z/(p^e), +, 0)$，即 $Z/(p^e)$ 的加群，到 U 的一个群同态．$Z/(p^e)$ 上的所有特征标组成的集合记为 $[Z/(p^e)]^v$，构成了一个 Abel 群．因此满足一般乘法群的特征标所满足的性质[15,16]．若令 $\chi_k = e^{2k\alpha\pi i/p^e}$，$a \in Z/(p^e)$，则 $[Z/(p^e)]^v = \{x_0, x_1, \cdots\cdots, x_{p^e-1}\}$，同时 $[Z/(p^e)]^v$ 还具有以下性质．

引理 3 若 $\chi_k \in [Z/(p^e)]^v$，$(0 \leqslant k \leqslant p^e - 1)$，则有

$$\sum_{b \in Z/(p^e)} \chi_k(bc) = \begin{cases} 0 & \text{若 } k \cdot c \not\equiv 0 \pmod{p^e} \\ p^e & \text{若 } k \cdot c \equiv 0 \pmod{p^e} \end{cases}$$

其中 $c \in Z/(p^e)$．

为证明结论，还需如下两个引理．

引理 4 设 $\underline{d} = (1,0,0,\cdots,0)^{tr}$，$f(x) \in P_n[Z/(p^e), x]$，则有 $[A_f^0\underline{d}, A_f^1\underline{d}, \cdots, A_f^{n-1}\underline{d}] = E_n$，其中 tr 为矩阵的转置运算，A_f 如 (3) 式定义，E_n 为 n 阶单位矩阵．

引理 5 设 $f(x) \in P_n[Z/(p^e), x]$，$\tilde{u} \in Q(Z/(p^e), f)$，且令 $S_k = \pi_{p^k}(\tilde{u})$，$(1 \leqslant k \leqslant e)$，则整数 t_1、t_2 和 $r(0 \leqslant t_1, t_2 \leqslant S_e - 1, 0 \leqslant r \leqslant e - 1)$ 满足

$$u_{t_1+i} - u_{t_2+i} \equiv 0 \pmod{p^{e-r}}, \quad (0 \leqslant i \leqslant n-1)$$

当且仅当 $S_{e-r} | t_1 - t_2$．

利用上述引理就可以证明以下定理．其中 $e(t) = e^{2t\pi i}$，t 为实数．

定理 14 若 $f(x) \in P_n[Z/(p^e), x]$，$\tilde{u} \in Q(Z/(p^e), f)$，$R_e = \pi_{p^e}(f)$，$S_l = \pi_{p^l}(\tilde{u})$，$(1 \leqslant l \leqslant e)$，则对任给的 $\chi_k \in [Z/(p^e)]^v$，$(k \not\equiv 0)$ 和 $h \in Z$，有

$$\left| \sum_{t=t}^{t_0+S_e-1} \chi_k(u_t) e\left(\frac{ht}{S_e}\right) \right| \leqslant \left(\frac{S_e}{S_{e-r}}\right)\left(\frac{S_{e-r}}{R_e}\right)^{1/2} \cdot p^{en/2}$$

其中 $t_0 \geqslant 0$，r 是满足 $k \equiv 0 \pmod{p^r}$ 的最大正整数．特别

$$\left| \sum_{t=t_0}^{t_0+S_e-1} \chi_k(u_t) \right| \leqslant \left(\frac{S_e}{S_1}\right)\left(\frac{S_1}{R_e}\right)^{1/2} \cdot p^{en/2}$$

有了以上准备后，即可得关于 $Z_{p^e}(b:\tilde{u})$ 的如下定理．

定理 15 若 $f(x) \in P_n[Z/(p^e), x]$，$\tilde{u} \in Q(Z/(p^e), f)$，其它记号同前，则任给 $b \in Z/(p^e)$，有 $|Z_{p^e}(b:\tilde{u}) - S_e/p^e| \leqslant (1 - 1/p^e)(S_e/S_1)(S_1/R_e)^{1/2} \cdot p^{en/2}$．

定理 16 若 $f(x) \in P_n[Z/(p^e), x]$ 是源不可约多项式，则有

$$|Z_{p^e}(b:\tilde{u}) - S_e/p^e| \leqslant (1 - 1/p^e) \cdot p^{en/2}$$

定理 17 若 $f(x) \in P_n[Z/(p^e), x]$ 是拟不可约多项式，且 $\tilde{u} \in Q(Z/(p^e), f)$ 满足 $u_0 \not\equiv 0 \pmod{p}$，则有 $|Z_{p^e}(b:\tilde{u}) - S_e/p^e| \leqslant (1 - 1/p^{e/2}) \cdot p^{en/2}$．

六、结 束 语

从本文结果可以看出 $Z/(m)$ 上的线性递归序列有许多好的性质，这为编码和密码

学的应用提供了方便．但是关于这一课题还有许多问题没有解决，有待进一步研究．

本文的工作得到了导师肖国镇教授以及课题组周锦君教授，奚邦余老师，王增法，戚文峰等同事的许多帮助和支持，在此向他们表示衷心的感谢．

附　　录

定理 7 的证明

用归纳法可以证明序列 $f_1(x)$，$g_1(x)$，$f_2(x)$，$g_2(x)$，$\cdots$，$f_{e-1}(x)$，$g_{e-1}(x)$ 的存在性和唯一性．

设 $n=\deg f_0(x)$，若 $\deg F(x)=N$，则 $\deg g_0(x)=N-n$．显然，$k=0$ 时结论成立，若 $k=r$ 时命题依然成立，我们将构造出满足定理条件的多项式 $f_{r+1}(x)$ 和 $g_{r+1}(x)$，从而证明这种序列的存在性．由于 $F(x)$，$f_r(x)$，$g_r(x)$ 均为首一多项式，且 $F(x)=f_r(x)g_r(x)\pmod{p^{r+1}}$，所以存在 $h(x)\in Z/(p)[x]$，$\deg h(x)<N$，使得

$$F(x)-f_r(x)g_r(x)=p^{r+1}\cdot h(x)\pmod{p^{r+2}} \tag{A1}$$

又因为 $(f_0(x),g_0(x))=1$，因此存在多项式 $u(x)$、$v(x)\in Z/(p)[x]$，使得

$$u(x)f_0(x)+v(x)g_0(x)=1\pmod{p}$$

用 $f_r(x)$ 除以 $h(x)\cdot v(x)$，可得多项式 $p(x)$，$r(x)\in Z/(p)[x]$，且 $\deg r(x)<\deg f_r(x)=n$，（其中约定 0 多项式的阶数为 $-\infty$），使 $h(x)v(x)=f_r(x)p(x)+r(x)\pmod{p}$．令 $q(x)=r(x)$，$m(x)=h(x)u(x)+p(x)g_r(x)$，由于 $f_r(x)=f_0(x)\pmod{p}$，$g_r(x)=g_0(x)\pmod{p}$，所以可验证有

$$m(x)f_r(x)+q(x)g_r(x)=h(x)\pmod{p} \tag{A2}$$

并且 $\deg q(x)=\deg r(x)<\deg f_r(x)=n$．同样，由于 $\deg h(x)<N$，$\deg q(x)g_r(x)=\deg q(x)+\deg g_r(x)<n+N-n=N$，所以，可由 (A2) 式得 $\deg m(x)+\deg f_r(x)=\deg m(x)f_r(x)<N$，即 $\deg m(x)<N-\deg f_r(x)=N-n=\deg g_r(x)$．

令

$$f_{r+1}(x)=f_r(x)+p^{r+1}\cdot q(x),\quad g_{r+1}(x)=g_r(x)+p^{r+1}\cdot m(x) \tag{A3}$$

则有如下结论：

(1) 由 (A3) 式可得 $f_{r+1}(x)=f_r(x)\pmod{p^{r+1}}$，$g_{r+1}(x)=g_r(x)\pmod{p^{r+1}}$；(2) 由 $\deg q(x)<\deg f_r(x)$，$\deg m(x)<\deg g_r(x)$ 和 (A3) 式，可得 $f_{r+1}(x)$，$g_{r+1}(x)$ 均为首一多项式，且 $\deg f_{r+1}(x)=\deg f_r(x)$，$\deg g_{r+1}(x)=\deg g_r(x)$；(3) 由 (A1)、(A2) 和 (A3) 式经过推导[12]，可得 $f_{r+1}(x)g_{r+1}(x)=[f_r(x)+p^{r+1}\cdot q(x)][g_r(x)+p^{r+1}\cdot m(x)]=F(x)\pmod{p^{r+2}}$．

综上所述，用归纳法证明了 $f_{r+1}(x)$ 和 $g_{r+1}(x)$ $(0\leqslant r\leqslant e-2)$ 的存在性．

对于唯一性，假设 $f'_{r+1}(x)$，$g'_{r+1}(x)$ 亦满足定理条件，即

$$f'_{r+1}(x)=f_r(x)\pmod{p^{r+1}},\quad g'_{r+1}(x)=g_r(x)\pmod{p^{r+1}} \tag{A4}$$

且

$$f'_{r+1}(x)g'_{r+1}(x)=F(x)=f_{r+1}(x)g_{r+1}(x)\pmod{p^{r+2}} \tag{A5}$$

由 (A4) 式可得

$$\begin{aligned} f'_{r+1}(x) &= f_r(x) + p^r \cdot t(x) \quad (\mathrm{mod}\, p^{r+2}) \\ g'_{r+1}(x) &= g_r(x) + p^r \cdot s(x) \quad (\mathrm{mod}\, p^{r+2}) \end{aligned} \tag{A6}$$

式中 $t(x)$, $s(x) \in Z/(p)[x]$, 由此 $\deg t(x) < n$, $\deg s(x) < N - n$, 将 (A6) 和 (A3) 式代入 (A5) 式可得 $f_r(x)g_r(x) + p^{r+1}[t(x)g_r(x) + s(x)f_r(x)] = f_r(x)g_r(x) + p^{r+1}[q(x)g_r(x) + m(x) \cdot f_r(x)] \ (\mathrm{mod}\, p^{r+2})$. 解得 $g_0(x)[t(x) - q(x)] = f_0(x)[m(x) - s(x)] \ (\mathrm{mod}\, p)$. 但是 $[f_0(x), g_0(x)] = 1$, 所以有 $f_0(x) \mid t(x) - q(x)$, $g_0(x) \mid m(x) - s(x) \ (\mathrm{mod}\, p)$. 而 $\deg(t(x) - q(x)) < \deg f_0(x)$, $\deg(m(x) - s(x)) < \deg g_0(x)$, 所以 $t(x) = q(x)$, $s(x) = m(x)$, $(\mathrm{mod}\, p)$. 由 (A3) 式和 (A6) 式可得

$$f'_{r+1}(x) = f_{r+1}(x), \quad g'_{r+1}(x) = g_{r+1}(x), \quad (\mathrm{mod}\, p^{r+2})$$

这样，唯一性得证.

通过上述证明，可得 $f_r(x)$ 和 $g_r(x)$，从而源多项式的构造并不困难，所给的算法仅依赖于 $Z[x]$ 上的 Euclidean 除法.

参 考 文 献

[1] E. R. Berlekamp, Algebra Coding Theory, MacGraw-Hill, New York, (1986).

[2] R. A. Rueppel, Analysis and Design of Stream Ciphers, Springer-Verlag, Berlin Heidelberg, (1986).

[3] C. Ronse, Feedback Shift Register, Lecture Notes in Computer Science, Springer-Verlag, Berlin Heidelberg, (1984).

[4] N. Zieler, *J. Soc. Indust. Appl. Math.*, 7(1959) 3, 37—48.

[5] 李献刚、肖国镇，椭圆曲线与序列密码，1989年全国信息论与通讯理论学术讨论会报告，青岛，1989年10月.

[6] J. A. Reeds, H. J. A. Sloane, Shift Register Synthesis (Module m). Math. and Statistic Research Center, Bell Lab., Murray Hill, NJ07974.

[7] I. F. Blake, *Inform. & Contr.* 29, (1975), 295—300.

[8] Eugene Spiegel, *Inform. & Control*, 35, (1977), 48—51.

[9] 周锦君、戚文锋，Z/(m)上线性递归序列的若干特性，国外通信保密研讨会会议录，襄樊，1987年 第187—201页.

[10] 陈立东，整数环上线性递归序列的分析，第三届全国密码学会会议录，西安，1988年，第 29—35 页.

[11] 李献刚，中国剩余定理与 $Z/(m)$ 上的递归序列，1989 年全国信息论与通讯理论学术讨论会报告，青岛，1989年.

[12] Li Xiangang, The Linear Recurring Sequences over Residue Class Ring Z/(m), 1990 IEEE International Symposium on Information Theory, San Diego, California, Jan. 14, (1990).

[13] 李献刚，$Z/(m)(x)$ 上的一个定理及其应用，1989年全国首届青年通信学术会议会议录，北京，1989 年 11 月 第 67—70 页.

[14] N. Koblitz, P-adic Numbers, P-adic Analysis, and Zeta-Functions, 2nd ed., Springer-Verlag, (1984).

[15] R. Lidl, N. Niederreiter, Finite Fields, Addison-Wesley Publishing Company, (1983).

[16] K. Ireland, M. Rosen, A Classical Introduction to Modern Number Theory, Springer-Verlag, (1982).

DISCUSSION ON LINEAR RECURRING SEQUENCES OVER $Z/(m)$

Li Xiangang

(Zhengzhou Engineering & Technical Institute, Zhengzhou)

Abstract The problems about the periods, the circle numbers, the distribution properties of the linear recurring sequences over $Z/(m)$ and the polynomials in $Z/(m)$ $[x]$ are discussed.

Key words Linear recurring sequence; Oriiginal (Quasi)-polynomial; Original (quasi) m-sequence; Period