文章编号:2095-0411(2017)06-0076-07

环 $Z/(p^eq)$ 上本原序列模整数的保熵性

孙霓刚,汪伟昕

(常州大学 信息科学与工程学院,江苏 常州 213164)

摘要:本原序列构造的算法可以有效抵抗面向比特的攻击,特别是抵抗代数攻击和快速相关攻击。针对环 $Z/(p^eq)$ 上由次数为 n 的本原多项式生成的本原序列,利用中国剩余定理和梯度法,构造了使其模 m 后保熵性成立的充分条件。分析表明,对于给定的 p,q 和 e,当 n 足够大时,本原序列模 m 后保熵性的充分条件一直成立。

关键词:整数剩余环;线性递归序列;本原序列;本原多项式

中图分类号:O 621.3 **文献标志码**:A **doi**:10.3969/j.issn.2095-0411.2017.06.011

On the Distinctness of Primitive Sequences Over $Z/(p^eq)$ Modulo Integers

SUN Nigang, WANG Weixin

(School of Information Science and Engineering, Changzhou University, Changzhou 213164, China)

Abstract: Primitive sequences have a significant contribution to algorithm's resistance against bit-oriented cryptographic attacks, including algebraic attacks and fast correlation attacks. This paper studied the primitive sequences generated by a primitive polynomial of degree n over $Z/(p^eq)$, utilizing the Chinese Remainder Theorem and Gradient Method. This article provided a sufficient condition to ensure the primitive sequences are pairwise distinct modulo m. Analysis showed that, for a given p, q and e, the sufficient condition for the entropy preserving property of the primitive sequence modulo m has been established.

Key words: integer residue rings; linear recurring sequences; primitive sequences; primitive polynomial

线性递归序列在脉冲响应和数字通信系统中有着很重要的作用,其本原的线性递归序列因其更加良好的性质而特别的重要。例如,3GPP 流密码算法 ZUC[1]就是采用 $Z/(2^{31}-1)$ 上的本原序列作为其驱动序列。密码分析[1]表明这类驱动序列构造出的算法能够有效的抵抗面向比特攻击,其中包括快速相关攻击,代数攻击等。

收稿日期:2017-04-06。

基金项目:国家自然科学基金资助项目(61103172)。

作者简介:孙霓刚(1978—),男,上海人,博士,副教授,主要从事通信安全、密码学研究。

对于整数 a 和一个大于等于 2 的正整数 b，用$[a]_{\mathrm{mod}\,b}$表示 a 模 b 的最小非负剩余。类似地，对于一个整数序列 $a=(a(t))_{t\geqslant 0}$，有$[a]_{\mathrm{mod}\,b}=([a(t)]_{\mathrm{mod}\,b})_{t\geqslant 0}$。环 $Z/(2^{31}-1)$上本原序列的之所以有上述良好的性质是因为其模 2 的保熵性[2]，也就是说对于环 $Z/(2^{31}-1)$上由本原多项式导出的本原序列 a 和 b，有 a=b 当且仅当$[a]_{\mathrm{mod}\,2}=[b]_{\mathrm{mod}\,2}$。对于环 $Z/(2^e-1)$这种更一般的情况，其中 $e\geqslant 2$ 是正整数，大量的实验数据表明，$Z/(2^e-1)$上次数 n≥2 的本原多项式生成的本原序列应该是模 2 保熵的，但是在理论上提供一个证明却十分困难。

通过研究，环 $Z/(2^e-1)$上保熵性的证明不比研究一般整数剩余环 $Z/(N)$来的简单，特别是对于一些特定的 e[3]，其中 N 是一个奇整数。这类问题的解决主要依靠 N 的整数分解，对于 N 是素数幂的情况，环 $Z/(N)$上本原序列的保熵性已经得到完美的解决[3]。

定理 1[2]　令 p^e 为奇素数幂整数，$f(x)$是环 $Z/(p^e)$上次数为 $n\geqslant 2$ 的本原多项式。那么有 $a=b$ 当且仅当$[a]_{\mathrm{mod}\,m}=[b]_{\mathrm{mod}\,m}$，其中 a 和 b 由环 $Z/(p^e)$上 $f(x)$生成的本原序列，且 m 至少有一个不同于 p 的素因子。

除此之外，在文献[4-8]，人们针对 N 不含平方因子的情况进行了广泛而深入的研究。对于 $N=p^eq$ 的情况，在文献[9]中，给出了环 $Z/(p^eq)$导出的本原序列模 2 保熵性成立的充分条件。本文利用了中国剩余定理以及梯度法[10]将文献[9]中模 2 保熵性推广到了模 m 的情况，其中 m 是大于 1 的整数且 $m\nmid p^eq$。

1　本原多项式与本原序列

令 N 为一个大于 1 的整数，如果有 $Z/(N)$上的序列 a 满足

$$a(i+n)=[c_{n-1}a(i+n-1)+\cdots+c_1a(i+1)+c_0a(i)]_{\mathrm{mod}\,N}$$

式中 i 是大于等于 1 的整数，n 是正整数且 $c_0,c_1\cdots c_{n-1}\in Z/(N)$是常系数，那么 a 被称为是由 $Z/(N)$上次数为 n 的多项式 $f(x)=x^n-c_{n-1}x^{n-1}-\cdots-c_0$ 生成的线性递归序列，$f(x)$为序列 a 的特征多项式，序列 a 特征多项式中次数最小被称为是最小多项式。为了方便叙述，通常将 $Z/(N)$上由 $f(x)$生成的线性递归序列的集记为 $G(f(x),N)$。

令 $f(x)$为 $Z/(N)$上次数为 n 首一的多项式，如果 $f(0)$是 $Z/(N)$上可逆元素，也就是说 $\gcd(f(0),N)=1$，那么存在一个正整数 T，使得 x^T-1在 $Z/(N)[x]$上整除 $f(x)$。满足上述条件最小整数 T 被称为 $Z/(N)$上 $f(x)$的周期，记为 $\mathrm{per}(f(x),N)$。当 $N=p^e$ 是一个素数幂整数，从文献[9]有 $\mathrm{per}(f(x),p^e)\leqslant p^{e-1}(p^n-1)$。如果 $\mathrm{per}(f(x),p^e)=p^{e-1}(p^n-1)$，那么 $f(x)$被称为 $Z/(p^e)$上次数 n 的本原多项式。当 a 是由 $Z/(p^e)$上本原多项式生成的序列且$[a]_{\mathrm{mod}\,p}$是一个非 0 序列，那么 a 称为 $Z/(p^e)$上的本原序列。

当 N 是一个任意整数时，假设 $N=p_1^{e_1}\,p_2^{e_2}\cdots p_r^{e_r}$ 是 N 的典范因子分解。如果对于 $i\in\{1,2,\cdots,r\}$，$f(x)\ \mathrm{mod}\,p_i^{e_i}$ 是 $Z/(p_i^{e_i})$上次数为 n 的本原多项式，那么称 $f(x)$是 $Z/(N)$上次数为 n 的本原多项式。当 a 是由 $Z/(N)$上次数为 n 本原多项式生成的序列，而且对于任意　$i\in\{1,2,\cdots,r\}$，$[a]_{\mathrm{mod}\,p_i}$ 都是非 0 序列，那么 a 是由 $Z/(N)$上的本原序列，且$[a]_{\mathrm{mod}p_1^{e_i}}$ 是 $Z/(p_i^{e_i})$上本原序列。同样为了叙述方便，通常将 $Z/(N)$上由本原多项式 $f(x)$生成的本原序列的集记为 $G'(f(x),N)$。

2　环 $Z/(p^e)$ 上序列的元素分布

令 p^e 为一个素数幂整数，对于 $Z/(p^e)$上的序列 $a=(a(t))_{t\geqslant 0}$，可以将 $a(t)$写成

$$a(t)=a_0(t)+a_1(t)\cdot p+\cdots+a_{e-1}(t)\cdot p^{e-1}$$

其中对于任意 $i\in\{0,1,\cdots,e-1\}$，有 $a_i(t)\in\{0,1,\cdots,p-1\}$，则称 a_i 为 a 的第 i 权位序列。

定义 1 如果 $f(x)$ 是 $Z/(p)$ 上次数为 n 的不可约多项式,那么首一多项式 $f(x)$ 是 $Z/(p^e)$ 上次数为 n 的基本不可约多项式。

根据上述定义,以下给出 $Z/(p^e)$ 上基本不可约多项式生成的线性递归序列元素分布的性质。

引理 1[11] 令 $f(x)$ 是 $Z/(p^e)$ 上次数为 $n\neq 2$ 的本原多项式,$a\in G'(f(x),p^e)$ 且 $a_0\neq 0$。如果

$$\mathrm{per}(f(x),p)\geqslant (p^e-1)p^{n/2+e-1}$$

那么 $Z/(p^e)$ 中每一个元素至少在 a 出现一次。

对于任意一个序列 $a=(a(t))_{t\geqslant 0}$ 和一个正整数 s,记 $a^{(s)}$ 为序列 a 的 s 采样序列,即 $a^{(s)}=(a(st))_{t\geqslant 0}$。

引理 2[9] 令 p^e 为一个素数幂整数,$f(x)$ 是 $Z/(p^e)$ 上次数为 n 的本原多项式。令 $a\in G'(f(x),p^e)$,s 是一个正整数,如果有

$$\frac{p^n-1}{\gcd(p^n-1,s)}>p^{\frac{n}{2}}$$

那么 $Z/(p^e)$ 上 $a^{(s)}$ 的最小多项式 $g(x)$ 只和 $f(x)$ 相关而且是一个唯一的次数为 n 基本不可约多项式。更多的有

$$\mathrm{per}(g(x),p^e)=\frac{p^{e-1}(p^n-1)}{\gcd(p^{e-1}(p^n-1),s)}$$

且 $$\mathrm{per}(g(x),p)=\frac{p^n-1}{\gcd(p^n-1,s)}$$

结合引理 1 和引理 2,可以推出以下的引理 3。

引理 3 $f(x)$ 是 $Z/(p^e)$ 上次数为 $n\geqslant 2$ 的本原多项式且 $a\in G'(f(x),p^e)$。令 s 是一个正整数,如果有

$$\frac{p^n-1}{\gcd(p^n-1,s)}\geqslant (p^e-1)p^{n/2+e-1}$$

那么 $Z/(p^e)$ 中每一个元素至少在 $a^{(s)}$ 出现一次。

令 $a=(a(t))_{t\geqslant 0}$ 和 $b=(b(t))_{t\geqslant 0}$ 是 $Z/(p^e)$ 上的序列。如果存在不全为 0 的 $u,v\in Z/(p^e)$,满足 $[u\cdot a+v\cdot b]_{\mathrm{mod}\ p^e}=0$,即对于任意的 $t\geqslant 0$,有 $[u\cdot a(t)+v\cdot b(t)]_{\mathrm{mod}\ p^e}=0$,那么称 a 和 b 在 $Z/(p^e)$ 线性相关。特别地,当 $e=1$ 时,如果 a 和 b 在 $Z/(p)$ 线性相关且 $b\neq 0$,那么有 $a=[\lambda\cdot b]_{\mathrm{mod}\ p}$,其中 $\lambda\in Z/(p)$。然后,对于 $e>1$ 的情况下,这个推论并不成立。

接下来给出 $Z/(p^e)$ 上 2 个线性不相关序列元素分布的性质。

引理 4[12] $f(x)$ 是 $Z/(p^e)$ 上次数为 n 的基本不可约多项式,$a,b\in G(f(x),p^e)$ 且 a,b 在 $Z/(p^e)$ 是线性无关的序列,如果有

$$\mathrm{per}(f(x),p)\geqslant (p^{2e}-1)p^{n/2+e-1}$$

那么对于任意 $u,v\in Z/(p^e)$,存在 $t\geqslant 0$ 满足 $a(t)=u,b(t)=v$。

结合引理 2 和引理 4,可以得出以下引理 5。

引理 5 $f(x)$ 是 $Z/(p^e)$ 上次数为 $n\geqslant 2$ 的本原多项式,$a,b\in G'(f(x),p^e)$。令 s 为一个正整数,且 $a^{(s)},b^{(s)}$ 在 $Z/(p^e)$ 上线性无关。如果有

$$\frac{p^n-1}{\gcd(p^n-1,s)}\geqslant (p^{2e}-1)p^{n/2+e-1}$$

那么对于任意 $u,v\in Z/(p^e)$,存在 $t\geqslant 0$ 满足 $a^{(s)}(t)=u,b^{(s)}(t)=v$。

3　环 $Z/(p^eq)$ 上本原序列模 m 的保熵性

在本节中，定义 p，q 为确定的不同的奇素数，e，m 为大于 1 的正整数且 $m \nmid p^eq$。在接下来的定理 2 中，给出主要结论。

定理 2　$f(x)$ 是 $Z/(p^eq)$ 上次数为 $n \geqslant 2$ 的本原多项式。如果有以下 2 个条件成立，

条件 1：
$$\frac{p^n-1}{\gcd(p^n-1,q^n-1)} \geqslant (p^e-1)p^{n/2+e-1}$$

条件 2：
$$\frac{q^n-1}{\gcd(q^n-1,p^{e-1}(p^n-1))} \geqslant (q^2-1)q^{n/2}$$

那么对于 $a,b \in G(f(x),p^eq)$，$a=b$ 当且仅当 $[a]_{\bmod m}=[b]_{\bmod m}$。

证明　定理的必要性显然成立，因此只需要证明其充分性，即 $[a]_{\bmod m}=[b]_{\bmod m}$ 可以推出 $a=b$。

令 $a,b \in G(f(x),p^eq)$ 是 2 个不同的本原序列，且有 $[a]_{\bmod m}=[b]_{\bmod m}$。利用中国剩余定理有

$$a=[q\cdot u_a+p^e\cdot v_a]_{\bmod p^eq}$$
$$b=[q\cdot u_b+p^e\cdot v_b]_{\bmod p^eq}$$

式中 $u_a,u_b \in G(f(x),p^e)$，$v_a,v_b \in G(f(x),q)$。

令 $m_1=\dfrac{m}{\gcd(m,p^e)}$，$m_2=\dfrac{m}{\gcd(m,q)}$，有以下 3 种情况：

第 1 种情况：$u_a=u_b$ 且 $v_a \neq v_b$。

利用定理 1，存在 $t \geqslant 0$ 满足

$$[v_a(t)]_{\bmod m_1} \neq [v_b(t)]_{\bmod m_1}$$

令 $c=[u_a(t+s)]_{s\geqslant 0}$ 是 u_a 的左移 t 位序列，有 $c \in G(f(x),p^e)$，同时令 $d=(u_a(t+k\cdot(q^n-1)))_{k\geqslant 0}$ 是 c 的 q^n-1 采样。那么利用条件 1 和引理 3，存在整数 $k^* \geqslant 0$ 满足 $d(k^*)=0$，也就是说

$$u_a(t+k\cdot(q^n-1))=u_b(t+k\cdot(q^n-1))=0。$$

因此序列 v_a,v_b 的周期为 q^n-1，那么有

$$a(t+k\cdot(q^n-1))=p^ev_a(t+k\cdot(q^n-1))=p^ev_a(t),$$
$$b(t+k\cdot(q^n-1))=p^ev_b(t+k\cdot(q^n-1))=p^ev_b(t)。$$

那么有 $[p^ev_a(t)]_{\bmod m}=[p^ev_b(t)]_{\bmod m}$，假设 $p^ev_a(t) \geqslant p^ev_b(t)$，于是就有 $[p^ev_a(t)-p^ev_b(t)]_{\bmod m}=0$，也就是

$$\frac{p^e}{\gcd(m,p^e)}[\gcd(m,p^e)(v_a(t)-v_b(t))]_{\bmod m}=0$$

推出

$$[\gcd(m,p^e)(v_a(t)-v_b(t))]_{\bmod m}=0$$

也就是说 $[(v_a(t)-v_b(t))]_{\bmod m_1}=0$，与假设矛盾。

第 2 种情况：· $u_a \neq u_b$ 且 $v_a=v_b$。

利用定理 1，存在 $t \geqslant 0$ 满足

$$[u_a(t)]_{\bmod m_2} \neq [u_b(t)]_{\bmod m_2}$$

利用情况 1 中的方法，构造 $d=(v_a(t+k\cdot p^{e-1}(p^n-1)))_{k\geqslant 0}$，同时应用条件 1 和引理 3，存在整数 $k^* \geqslant 0$，满足 $d(k^*)=0$，也就是说

$$v_a(t+k\cdot p^{e-1}(p^n-1))=v_b(t+k\cdot p^{e-1}(p^n-1))=0$$

和情况 1 一样，可以推出

$$[u_a(t)]_{\bmod m_2}=[u_b(t)]_{\bmod m_2}$$

与假设矛盾。

第 3 种情况:$u_a \neq u_b$ 且 $v_a \neq v_b$。

利用定理 1,存在 $t \geqslant 0$ 满足

$$[u_a(t)]_{\mathrm{mod}\, m_2} \neq [u_b(t)]_{\mathrm{mod}\, m_2}。$$

令

$$d_a = (v_a(t + k \cdot p^{e-1}(p^n - 1)))_{k \geqslant 0}$$

和

$$d_b = (v_b(t + k \cdot p^{e-1}(p^n - 1)))_{k \geqslant 0}$$

考虑以下 2 种子情况:

1) d_a 和 d_b 在 $Z/(p)$ 上线性独立

利用条件 2 和引理 5,存在 $k^* \geqslant 0$ 使 $d_a(k^*) = d_b(k^*) = 0$。

2) d_a 和 d_b 在 $Z/(p)$ 上线性相关

d_a 和 d_b 在 $Z/(p)$ 上线性相关,且 $d_b \neq 0$,那么对于 d_a 和 d_b 就有 $d_a = [\lambda \cdot d_b]_{\mathrm{mod}\, q}$,其中 $\lambda \in Z/(q)$。那么利用条件 2 和引理 2,存在 $k^* \geqslant 0$ 使 $d_a(k^*) = 0$,因此 $d_b(k^*) = 0$。

结合上述所有情况,完成了证明。

注释 1 如果序列 a 和 b 在 $Z/(p^e q)$ 上线性无关,那么有序列 u_a 和 u_b 在 $Z/(p^e)$ 上线性无关和序列 v_a 和 v_b 在 $Z/(q)$ 上线性无关。

证明 为了不失一般性,令序列 u_a 和 u_b 在 $Z/(p^e)$ 上线性相关,那么存在不全为 0 的 k_a, k 满足

$$[k_a \cdot u_a + k_b \cdot u]_{\mathrm{mod}\, p^e} = 0$$

那么有

$$[k_a q \cdot [q \cdot u_a + p^e \cdot v_a]_{\mathrm{mod}\, p^e q} + k_b q \cdot [q \cdot u_b + p^e \cdot v_b]_{\mathrm{mod}\, p^e q}]_{\mathrm{mod}\, p^e q} =$$
$$[k_a q \cdot [q \cdot u_a + p^e \cdot v_a] + k_b q \cdot [q \cdot u_b + p^e \cdot v_b]]_{\mathrm{mod}\, p^e q} =$$
$$[k_a q \cdot u_a + k_b q \cdot u]_{\mathrm{mod}\, p^e q}$$

其中 $k_a q, k_b q \in Z/(p^e q)$。

注释 2 在定理 2 的条件下,对于序列 $a, b \in G(f(x), p^e q)$,如果 a 和 b 在 $Z/(p^e q)$ 上线性不相关,那么对于任意的 2 个值 $k^1, k^2 \in Z/(p^e q)$,存在整数 $t \geqslant 0$ 有 $a(t) = k^1, b(t) = k^2$。

证明 利用定理 2 和注释 1 有

$$k^1 = [q \cdot k_u^1 + p^e \cdot k_v^1]_{\mathrm{mod}\, p^e q}$$
$$k^2 = [q \cdot k_u^2 + p^e \cdot k_v^2]_{\mathrm{mod}\, p^e q}$$

其中 $k_u^1, k_v^1 \in \mathrm{Z/(p^e)}$ 和 $k_u^2, k_v^2 \in \mathrm{Z/(q)}$。利用引理 4,存在整数 $t_0 \geqslant 0$ 满足 $u_a(t_0) = k_u^1, u_b(t_0) = k_u^2$。同时利用引理 5,存在整数 $k^* \geqslant 0$ 满足 $v_a(t_0 + k^*(q^n - 1)) = k_v^1, v_b(t_0 + k^*(q^n - 1)) = k_v^2$。根据以上结论令 $t = t_0 + k^*(q^n - 1)$,有 $a(t) = k^1, b(t) = k^2$。

注释 3 在定理 2 中的条件下,对于 $a \in G(f(x), p^e q)$ 有

$$\mathrm{per}([a]_{\mathrm{mod}\, m}) = \mathrm{per}(a) = l\mathrm{cm}(p^{e-1} \cdot (p^n - 1), q^n - 1)$$

其中 $\mathrm{per}(a)$ 表示序列 a 的周期。

显然有 $\mathrm{per}(a) = \mathrm{lcm}(p^{e-1} \cdot (p^n - 1), q^n - 1)$,根据定理 2 又有 $\mathrm{per}([a]_{\mathrm{mod}\, m}) \leqslant \mathrm{per}(a)$。令 $(a(t + k))_{t \geqslant 0}$ 是序列 a 的 k 移位序列,那么有对于 $0 < k < \mathrm{per}(a)$,有 $(a(t + k))_{t \geqslant 0} \neq a$,又根据定理 2 有 $[(a(t + k))_{t \geqslant 0}]_{\mathrm{mod}\, m} \neq [a]$ 表明 $r([a]_{\mathrm{mod}\, m}) \geqslant \mathrm{per}(a)$,从而可以得到 $\mathrm{per}([a]_{\mathrm{mod}\, m}) = \mathrm{per}(a)$。

注释 4 当 $n \leqslant 2(2e - 1)$ 时,条件 1 是不成立的,事实上当 $n \leqslant 2(2e - 1)$ 时,有

$$\frac{p^n-1}{\gcd(p^n-1,q^n-1)}<p^{n/2}\leqslant\frac{p^{n/2+e-1}}{2}<(p^e-1)p^{n/2+e-1}$$

接下来，给出定理 2 中条件 1 和条件 2 的讨论，当 $e=3$ 时，表 1 中给出满足条件的 (p,q) 所占百分比，其中 p,q 满足 $3\leqslant p\neq q\leqslant \text{prime}(5\ 000)$，$\text{prime}(k)$ 表示第 k 个素数。

表 1　$3\leqslant p\neq q\leqslant$ prime(5 000) 满足条件 1 和 2 的 (p,q) 所占比例　%

n	$3\leqslant p\neq q\leqslant$ prime(5 000)	n	$3\leqslant p\neq q\leqslant$ prime(5 000)
11	85.810	21	99.999
12	0	22	99.984
13	99.949	23	99.999
14	99.536	24	99.939
15	99.931	25	99.999
16	99.609	26	99.999
17	99.998	27	99.998
18	99.735	28	99.997
19	99.999	29	99.999
20	99.909	30	99.603

以下给出对于给定的 p,q 和 e，当 n 足够大时，定理中条件 1 和条件 2 严格成立。

引理 6[13]　如果 a 和 b 是 2 个大于 1 乘法独立的正整数，那么对于任意实数 $\varepsilon>0$，存在 1 个整数 N_ε 满足

$$\gcd(a^n-1,b^n-1)<2^{n\varepsilon}$$

其中 $n>N_\varepsilon$。

利用引理 6 中的不等式，得到以下定理：

定理 3　对于给定的 p,q 和 e，那么存在一个整数 N，当 $n>N$ 成立时，定理 2 中的条件 1 和条件 2 严格成立。

证明　因为 p 和 q 是大于 1 乘法独立的整数，那么根据引理 6，有对于给定实数 $\varepsilon>0$，存在一个整数 N_ε 满足

$$\gcd(p^n-1,q^n-1)<2^{n\varepsilon}$$

其中 $n>N_\varepsilon$。因此有以下不等式成立

$$\frac{p^n-1}{\gcd(p^n-1,q^n-1)}>\frac{p^n-1}{2^{n\varepsilon}}\frac{q^n-1}{\gcd(q^n-1,p^{e-1}(p^n-1))}\geqslant$$

$$\frac{q^n-1}{p^{e-1}\gcd(q^n-1,p^n-1)}>\frac{q^n-1}{p^{e-1}2^{n\varepsilon}}$$

选择 $0<\varepsilon<\frac{1}{2}$，那么有

$$\lim_{n\to\infty}\frac{p^n-1}{2^{n\varepsilon}(p^e-1)p^{n/2+e-1}}=+\infty$$

$$\lim_{n\to\infty}\frac{p^n-1}{p^{e-1}2^{n\varepsilon}(q^2-1)q^{n/2}}=+\infty$$

因此存在一个整数 N'，当 $n>N'$ 时有

$$\frac{p^n-1}{2^{n\varepsilon}}>(p^e-1)p^{n/2+e-1}$$

$$\frac{q^n-1}{p^{e-1}2^{n\varepsilon}}>(q^2-1)q^{n/2}$$

令 $N=\max\{N_\varepsilon,N'\}$，定理 3 证毕。

4　结　论

针对环 $Z/(p^eq)$ 上由次数为 n 的本原多项式生成的本原序列，研究了其模 m 后保熵性成立的充分条件。结果表明，对于给定的 p,q 和 e，当 n 足够大时，该本原序列模 m 后保熵性的充分条件一直成立。

参考文献:

[1][s.n.]. ETSI/SAGE specification: specification of the 3GPP confidentiality and integrity algorithms 128-EEA3 & 128-EIA3,document 4:design and evaluation report, version: 2.0[EB/OL]. (2011-09-01)[2017-03-27]. http://zuc.dacas.cn/thread.aspx ID=2304.

[2]ZHU X Y, QI W F. On the distinctness of modular reductions of maximal length sequences modulo odd prime powers [J]. Mathematics of Computation, 2008, 77: 1623-1637.

[3]ZHENG Q X, QI W F, TIAN T. On the distinctness of modular reductions of primitive sequences over $Z/(2^{32}-1)$ [J]. Des Codes Cryptograph, 2014, 70(3): 359-368.

[4]CHEN H J, QI W F. On the distinctness of maximal length sequences over modulo 2[J]. Finite Fields & Their Applications, 2009, 15(1): 23-39.

[5]ZHENG Q X, QI W F. A new result on the distinctness of primitive sequences over $Z/(pq)$ modulo 2[J]. Finite Fields & Their Applications, 2011, 17(3): 254-274.

[6]ZHENG Q X, QI W F, TIAN T. On the distinctness of binary sequences derived from primitive sequences modulo square-free odd integers[J]. Information Theory IEEE Transactions on, 2013, 59(1): 680-690.

[7]ZHENG, Q X, QI W F. Further results on the distinctness of binary sequences derived from primitive sequences modulo square-free odd integers[J]. Information Theory IEEE Transactions on, 2013, 59(1): 4013-4019.

[8]HU Z, WANG L. Injectivity of compressing maps on the set of primitive sequences modulo square-free odd integers [J]. Cryptography & Communications, 2015, 7(4): 347-361.

[9]CHENG Y, QI W, ZHENG Q, et al. On the distinctness of primitive sequences over $Z/(p^rq)$ modulo 2[J]. Cryptography and Communications, 2016, 8(3): 371-381.

[10]YANG D, QI W F, ZHENG Q X. Further results on the distinctness of modulo 2 reductions of primitive sequences over $Z/(2^{32}-1)$[J]. Designs Codes & Cryptography, 2015, 74(2): 467-480.

[11]BYLKOV D N, KAMLOVSKI O V. Occurrence indices of elements in linear recurring sequences over primary residue rings[J]. Problems of Information Transmission, 2008, 44(2): 161-168.

[12]KAMLOVSKII O V. Frequency characteristics of linea r recurrence sequences over Galois rings[J]. Russian Academy of Sciences Sbornik Mathematics, 2009, 200(4): 31-52.

[13]BUGEAUD Y, CORVAJA P, ZANNIER U. An upper bound for the GCD of a^n-1 and b^n-1[J]. Mathematische Zeitschrift, 2003, 243(1): 79-84.

(责任编辑:李艳)