A new result on the distinctness of primitive sequences over $\mathbf{Z}/(pq)$ modulo 2*

Qun-Xiong Zheng and Wen-Feng Qi†

September 20, 2010

Abstract

Let $\mathbf{Z}/(pq)$ be the integer residue ring modulo pq with odd prime numbers p and q. This paper studies the distinctness problem of modulo 2 reductions of two primitive sequences over $\mathbf{Z}/(pq)$, which has been studied by H.J. Chen and W.F. Qi in 2009. First, it is shown that almost every element in $\mathbf{Z}/(pq)$ occurs in a primitive sequence of order $n > 2$ over $\mathbf{Z}/(pq)$. Then based on this element distribution property of primitive sequences over $\mathbf{Z}/(pq)$, previous results are greatly improved and the set of primitive sequences over $\mathbf{Z}/(pq)$ that are known to be distinct modulo 2 is further enlarged.

Keywords: integer residue rings, linear recurring sequences, primitive polynomials, primitive sequences, modular reduction

*This work was supported by NSF of China under Grant No. (61070178, 60833008).

†Qun-Xiong Zheng and Wen-Feng Qi are with the department of Applied Mathematics, Zhengzhou Information Science and Technology Institute, Zhengzhou, P.R.China. (e-mail: qunxiong_zheng@163.com and wenfeng.qi@263.net).

1 Introduction

For an integer $N \geq 2$, let $\mathbf{Z}/(N) = \{0, 1, \ldots, N-1\}$ be the integer residue ring modulo N, and for any integer a, let $[a]_{\mathrm{mod}\, N}$ denote the minimal nonnegative residue of a modulo N. Moreover, for an integer sequence $\underline{a} = (a(t))_{t\geq 0}$, denote $[\underline{a}]_{\mathrm{mod}\, N} = ([a(t)]_{\mathrm{mod}\, N})_{t\geq 0}$.

If a sequence $\underline{a} = (a(t))_{t\geq 0}$ over $\mathbf{Z}/(N)$ satisfies

$$a(i+n) = -\left(c_{n-1}a(i+n-1) + \cdots + c_1 a(i+1) + c_0 a(i)\right) \bmod N,\ i \geq 0 \tag{1}$$

with constant coefficients $c_0, c_1, \ldots, c_{n-1} \in \mathbf{Z}/(N)$, then $\underline{a}$ is called a linear recurring sequence of order n generated by $f(x)$ over $\mathbf{Z}/(N)$ (or $\underline{a}$ is a sequence of order n over $\mathbf{Z}/(N)$ in short), where $f(x) = x^n + c_{n-1}x^{n-1} + \ldots + c_0$. The set of sequences generated by $f(x)$ over $\mathbf{Z}/(N)$ is denoted by $G\left(f\left(x\right), N\right)$.

Let p be a prime number and e a positive integer. Every element $u \in \mathbf{Z}/(p^e)$ has a unique p-adic expansion as $u = u_0 + u_1 \cdot p + \ldots + u_{e-1} \cdot p^{e-1}$, where $u_i \in \{0, 1, \cdots, p-1\}$ and can be naturally seen as an element in $\mathbf{Z}/(p)$. Similarly, a sequence $\underline{a}$ over $\mathbf{Z}/(p^e)$ has a unique p-adic expansion as $\underline{a} = \underline{a}_0 + \underline{a}_1 \cdot p + \ldots + \underline{a}_{e-1} \cdot p^{e-1}$, where $\underline{a}_i$ is a sequence over $\{0, 1, \cdots, p-1\}$ and can be naturally seen as a sequence over $\mathbf{Z}/(p)$. $\underline{a}_i$ is called the i**th-level sequence** of $\underline{a}$ for $0 \leq i \leq e-1$ and $\underline{a}_{e-1}$ is also called the **highest level sequence** of $\underline{a}$.

A monic polynomial $f(x)$ over $\mathbf{Z}/(p^e)$ is called a **primitive polynomial** if the period of $f(x)$ over $\mathbf{Z}/(p^e)$, denoted by $per(f(x), p^e)$, is equal to $p^{e-1}(p^n - 1)$, that is $p^{e-1}(p^n - 1)$ is the minimal positive integer P such that $x^P - 1$ is divisible by $f(x)$ in $\mathbf{Z}/(p^e)[x]$. A sequence $\underline{a} = (a(t))_{t\geq 0}$ over $\mathbf{Z}/(p^e)$ is called a **primitive sequence (or maximal length sequence)** if $\underline{a}$ is generated by a primitive polynomial over $\mathbf{Z}/(p^e)$ and $\underline{a}_0 \neq \underline{0}$, where $\underline{a}_0$ is the 0th-level sequence of $\underline{a}$ and $\underline{0} = (0, 0, \ldots)$ is a constant sequence. The period of a primitive sequence $\underline{a}$ over $\mathbf{Z}/(p^e)$ is equal to $p^{e-1}(p^n - 1)$, i.e., $per\left(\underline{a}, p^e\right) = p^{e-1}(p^n - 1)$, see [1].

Let $\underline{a} = \underline{a}_0 + \underline{a}_1 \cdot p + \ldots + \underline{a}_{e-1} \cdot p^{e-1}$ be a primitive sequence over $\mathbf{Z}/(p^e)$ and $\varphi(x_0, \ldots, x_{e-1})$

be an e-variable function over $\mathbf{Z}/(p)$. Then $\varphi(\underline{a}_0, \ldots, \underline{a}_{e-1})$ is a sequence over $\mathbf{Z}/(p)$ and is called a compressing sequence derived from $\underline{a}$. Many cryptographical properties of such compressing sequences have been studied during the last 20 years [2]-[15], especially the distinctness of the compressing sequences [2], [3], [6], [8]-[11] and [14], that is, $\underline{a} = \underline{b}$ if and only if $\varphi(\underline{a}_0, \ldots, \underline{a}_{e-1}) = \varphi(\underline{b}_0, \ldots, \underline{b}_{e-1})$, where $\underline{a}$ and $\underline{b}$ are two primitive sequences generated by the same primitive polynomial over $\mathbf{Z}/(p^e)$. Obviously, for a given primitive polynomial $f(x)$ over $\mathbf{Z}/(p^e)$, if the compressing sequences of all primitive sequences generated by $f(x)$ are pairwise distinct, then there is a one-to-one correspondence between compressing sequences and primitive sequences, which implies that every compressing sequence preserves all the information of its original primitive sequences. Thus such compressing sequences are thought to be a good type of nonlinear sequences available for the design of stream cipher.

Recently, modular reduction, another compressing method of primitive sequences over $\mathbf{Z}/(p^e)$, is proposed and has attracted much attention. For example, the well known l-sequences, i.e., maximal length FCSR sequences, introduced by A. Klapper and M. Goresky in [17], are in fact modulo 2 reductions of primitive sequences of order 1 over $\mathbf{Z}/(p^e)$. In [16], the distinctness of modular reductions of primitive sequences over $\mathbf{Z}/(p^e)$ has been completely solved. It was shown that if $\underline{a}$ and $\underline{b}$ are two primitive sequences generated by a primitive polynomial of degree $n \geq 1$ over $\mathbf{Z}/(p^e)$, then $\underline{a} = \underline{b}$ if and only if $[\underline{a}]_{\bmod M} = [\underline{b}]_{\bmod M}$, where M is a positive integer and has a prime factor other than p. It can be seen that the operation of $\bmod M$ destroys the inherent structure of sequences over $\mathbf{Z}/(p^e)$, and in particular for $M = 2$, the compression ratio is very large and easy to implement.

Furthermore, in [18], the authors generalized the modular reductions of primitive sequences over $\mathbf{Z}/(p^e)$ to primitive sequences over every integer residue ring $\mathbf{Z}/(N)$, where N is an integer greater than 1. Before introduce their result, we first give the definitions of a primitive polynomial and a primitive sequence over $\mathbf{Z}/(N)$.

Definition 1 *Let N be an integer greater than 1 and $N = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_k^{e_k}$ be the canonical*

factorization of N. A monic polynomial $f(x)$ of degree n over $\mathbf{Z}/(N)$ is called a primitive polynomial if $f(x) \pmod{p_i^{e_i}}$ is a primitive polynomial of degree n over $\mathbf{Z}/(p_i^{e_i})$ for every $1 \le i \le k$. A sequence $\underline{a}$ of order n over $\mathbf{Z}/(N)$ is called a primitive sequence if $[\underline{a}]_{\bmod p_i^{e_i}}$ is a primitive sequence of order n over $\mathbf{Z}/(p_i^{e_i})$ for every $1 \le i \le k$.

With the above definition, it is easy to see that both the period of a primitive polynomial $f(x)$ of degree n over $\mathbf{Z}/(N)$ and the period of a primitive sequence of order n over $\mathbf{Z}/(N)$ are equal to $\operatorname{lcm}\left(p_1^{e_1-1}(p_1^n-1), \ldots, p_k^{e_k-1}(p_k^n-1)\right)$, that is

$$per\,(f(x), N) = per\,(\underline{a}, N) = \operatorname{lcm}\left(p_1^{e_1-1}(p_1^n-1), \ldots, p_k^{e_k-1}(p_k^n-1)\right).$$

For convenience, the set of primitive sequences generated by a primitive polynomial $f(x)$ over $\mathbf{Z}/(N)$ is denoted by $G'(f(x), N)$.

If N has at least two different prime factors, there indeed exist many primitive sequences of order 1 over $\mathbf{Z}/(N)$ such that their modular reductions are the same [18]. It is still open, however, whether the modular reductions of primitive sequences of order $n \ge 2$ over $\mathbf{Z}/(N)$ are distinct. In [18], the authors proved the following result for $n \ge 2$.

Theorem 2 *([18]) Let p and q be two odd prime numbers with $p < q$ and $f(x)$ be a primitive polynomial of degree $n \ge 2$ over $\mathbf{Z}/(pq)$. If the following two conditions are satisfied:*

(1) *there exist a positive integer S and a primitive element ξ in $\mathbf{Z}/(pq)$ such that*

$$x^S - \xi \equiv 0 \bmod (f(x), pq);$$

(2) *$(q-1)$ is not divisible by $(p-1)$ or $2(p-1)$ divides $(q-1)$,*

then for $\underline{a}, \underline{b} \in G'(f(x), pq)$, $\underline{a} = \underline{b}$ if and only if $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$.

In this paper, we also study the distinctness of primitive sequences over $\mathbf{Z}/(pq)$ modulo 2, and with our new result, the set of primitive sequences that can be proved to be distinct modulo 2 is greatly enlarged. First we estimate the element distribution of primitive sequences over $\mathbf{Z}/(pq)$. Experiments show that for most of the cases, our estimation implies

that every element in $\mathbf{Z}/(pq)$ occurs in a given primitive sequence of order $n > 2$ over $\mathbf{Z}/(pq)$. Based on the result of element estimation, we obtain a new sufficient condition on the distinctness of primitive sequences over $\mathbf{Z}/(pq)$ modulo 2 as follows.

Theorem 3 *Let p and q be two odd prime numbers with $p < q$ and $f(x)$ be a primitive polynomial of degree $n \geq 2$ over $\mathbf{Z}/(pq)$. Set $T = \mathrm{lcm}\,(p^n - 1, q^n - 1)$ and*

$$E = \begin{cases} \frac{(p-1)\cdot(q-1)\cdot(pq)^{\frac{n}{2}}}{1-\frac{p-1}{p^n-1}-\frac{q-1}{q^n-1}}, & \text{if } v_2\,(p^n-1) \neq v_2\,(q^n-1)\,; \\ \max\left\{\frac{(p-1)\cdot(q-1)\cdot(pq)^{\frac{n}{2}}}{1-\frac{p-1}{p^n-1}-\frac{q-1}{q^n-1}}, \left\lfloor \frac{q}{p} \right\rfloor \cdot \mathrm{lcm}\left(p^n-1, \frac{q^n-1}{q-1}\right)\right\}, & \text{if } v_2\,(p^n-1) = v_2\,(q^n-1)\,. \end{cases}$$

where $v_2\,(u)$ is the greatest nonnegative integer m such that 2^m divides u. If the following two conditions are satisfied:

(1) *there exist a positive integer S and an even number C in $\mathbf{Z}/(pq)$ such that*

$$x^S - C \equiv 0\,(\mathrm{mod}\, f(x), pq);$$

(2) $T > E$,

then for $\underline{a}, \underline{b} \in G'(f(x), pq)$, $\underline{a} = \underline{b}$ if and only if $[\underline{a}]_{\mathrm{mod}\,2} = [\underline{b}]_{\mathrm{mod}\,2}$.

The proportion of (n, p, q) satisfying the conditions of Theorem 3 is tested for different ranges of n, p and q, and results show that such proportion is very high. For example, the proportion is at least 93.756% for $2 \leq n \leq 31$ and $3 \leq p < q < 1000$, whereas the corresponding proportion of Theorem 2 is only 48.765% [18]. Moreover, the existence of S and C described in condition (1) of Theorem 3 is discussed. A sufficient condition is given in Corollary 17 for the existence of such S and C. Experiments show that for the same ranges of n, p and q, the proportion of (n, p, q) satisfying the conditions of Corollary 17 is also higher than that of Theorem 1 in [18], though the conditions of Corollary 17 are stronger than those of Theorem 3.

The rest of this paper is organized as follows. In Section 2 the element distribution of primitive sequences over $\mathbf{Z}/(pq)$ is estimated. Section 3 gives the proof of Theorem 3 and

discusses the number of primitive sequences satisfying the sufficient conditions given by Theorem 3.

2 Element distribution of primitive sequences over $\mathbf{Z}/(pq)$

In the following of the paper, suppose that p and q are two fixed odd prime numbers with $p < q$.

Let $\underline{a}$ be a periodic sequence over $\mathbf{Z}/(pq)$ with $T = per(\underline{a}, pq)$. For any fixed integer $s \in \mathbf{Z}/(pq)$, if there exists an integer $0 \leq t \leq T-1$ such that $a(t) = s$, then we say that the element s occurs in $\underline{a}$. Let $N\left(\underline{a}^T, s\right)$ denote the frequency of element s occurring in a complete period of the sequence $\underline{a}$, that is,

$$N\left(\underline{a}^T, s\right) = \#\left\{t \mid a(t) = s, 0 \leq t \leq T-1\right\}.$$

If $\underline{a}$ is a primitive sequence generated by a primitive polynomial of degree $n = 1$ over $\mathbf{Z}/(pq)$, then it is easy to see that not all elements in $\mathbf{Z}/(pq)$ occur in $\underline{a}$. However, as n increases, it seems that every element in $\mathbf{Z}/(pq)$ occurs in $\underline{a}$. In this section, we present a sufficient condition for this element distribution property.

Let $e_m(\cdot)$ be the canonical additive character over $\mathbf{Z}/(m)$ given by $e_m(a) = e^{2\pi ia/m}$, where $a \in \mathbf{Z}/(m)$. Then it is easy to see that the following lemma holds.

Lemma 4 *Let m be an integer greater than 1. Then for any integer c,*

$$\sum_{a=0}^{m-1} e_m(ca) = \begin{cases} m, & \text{if } m \mid c; \\ 0, & \text{otherwise.} \end{cases}$$

For any positive integer n, denote

$$(\mathbf{Z}/(pq))^n = \{(a_1, a_2, \ldots, a_n) \mid a_i \in \mathbf{Z}/(pq), 1 \leq i \leq n\}.$$

Lemma 5 *Let* $f(x) = x^n - (c_{n-1}x^{n-1} + \cdots + c_1 x + c_0)$ *be a primitive polynomial over* $\mathbf{Z}/(pq)$ *and let* $\mathbf{d} = (1, 0, \cdots, 0) \in (\mathbf{Z}/(pq))^n$. *Then* $\mathbf{d} \cdot A^m \neq \mathbf{d} \cdot A^k$ *for* $0 \leq m < k < \operatorname{lcm}(p^n - 1, q^n - 1)$, *where*

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ c_0 & c_1 & c_2 & c_3 & \cdots & c_{n-1} \end{bmatrix}. \tag{2}$$

Proof. Let $T = \operatorname{lcm}(p^n - 1, q^n - 1)$. Suppose there exist two integers m and k, $0 \leq m < k < T$ such that $\mathbf{d} \cdot A^m = \mathbf{d} \cdot A^k$. Then we have

$$\left(\mathbf{d} \cdot A^j\right) \cdot A^m = \left(\mathbf{d} \cdot A^j\right) \cdot A^k \text{ for } 0 \leq j \leq n-1 \tag{3}$$

Note that

$$\mathbf{d} \cdot A^j = (\underbrace{0, \ldots, 0}_{j}, 1, 0, \ldots, 0), 0 \leq j \leq n-1,$$

and so (3) implies that

$$A^m = A^k. \tag{4}$$

Let $\underline{d} = (d(t))_{t \geq 0}$ be a primitive sequence generated by $f(x)$ over $\mathbf{Z}/(pq)$ and $\mathbf{d}_t = (d(t), d(t+1), \cdots, d(t+n-1))$ be the t-th state of the sequence $\underline{d}$ for an integer $t \geq 0$. It follows from (1) that

$$\mathbf{d}_t^\tau = A^t \cdot \mathbf{d}_0^\tau,$$

where $\mathbf{d}^\tau$ is the transpose of $\mathbf{d}$. Then by (4) we have

$$\mathbf{d}_m^\tau = A^m \cdot \mathbf{d}_0^\tau = A^k \cdot \mathbf{d}_0^\tau = \mathbf{d}_k^\tau,$$

a contradiction to $per(\underline{d}, pq) = T$. Therefore $\mathbf{d} \cdot A^m \neq \mathbf{d} \cdot A^k$ for $0 \leq m < k < T$. ■

Lemma 6 *Let $\underline{a}$ be a primitive sequence generated by a primitive polynomial of degree $n \geq 2$ over $\mathbf{Z}/(pq)$ with period $T = \operatorname{lcm}(p^n - 1, q^n - 1)$. Then*

$$\left| \sum_{t=0}^{T-1} e_{pq}(a(t)) \right| \leq (pq)^{\frac{n}{2}} .$$

Proof. For any vector $\mathbf{b} = (b_0, b_1, \cdots, b_{n-1}) \in (\mathbf{Z}/(pq))^n$, let

$$\sigma(\mathbf{b}) = \sum_{t=0}^{T-1} e_{pq}(b_0 a(t) + b_1 a(t+1) + \cdots + b_{n-1} a(t+n-1)). \tag{5}$$

Note that

$$\begin{aligned} & e_{pq}(b_0 a(0) + b_1 a(1) + \cdots + b_{n-1} a(n-1)) \\ = \; & e_{pq}(b_0 a(T) + b_1 a(T+1) + \cdots + b_{n-1} a(T+n-1)), \end{aligned}$$

and so we obtain

$$\sigma(\mathbf{b}) = \sum_{t=0}^{T-1} e_{pq}(b_0 a(t+1) + b_1 a(t+2) + \cdots + b_{n-1} a(t+n)). \tag{6}$$

Assume $f(x) = x^n - (c_{n-1}x^{n-1} + \cdots + c_1 x + c_0)$. Then we have

$$a(t+n) = [c_0 a(t) + c_1 a(t+1) + \cdots + c_{n-1} a(t+n-1)]_{\bmod pq}, t \geq 0. \tag{7}$$

Hence, (6) and (7) yield

$$\begin{aligned} |\sigma(\mathbf{b})| &= \left| \sum_{t=0}^{T-1} e_{pq}(b_0 a(t+1) + b_1 a(t+2) + \cdots + b_{n-1} a(t+n)) \right| \\ &= \left| \sum_{t=0}^{T-1} e_{pq}\left(b_0 a(t+1) + b_1 a(t+2) + \cdots + b_{n-1}\left(\sum_{k=0}^{n-1} c_k a(t+k) \right) \right) \right| \\ &= |\sigma(b_{n-1}c_0, b_0 + b_{n-1}c_1, \cdots, b_{n-2} + b_{n-1}c_{n-1})| \\ &= |\sigma(\mathbf{b} \cdot A)|, \end{aligned}$$

where A is an $n \times n$ matrix over $\mathbf{Z}/(pq)$ of the form described in (2).

Recursively, we have

$$|\sigma(\mathbf{b})| = |\sigma(\mathbf{b} \cdot A)| = \left|\sigma\left(\mathbf{b} \cdot A^2\right)\right| = \cdots = \left|\sigma\left(\mathbf{b} \cdot A^{T-1}\right)\right|. \tag{8}$$

Therefore, it follows that

$$\begin{aligned}
& \sum_{\mathbf{b}\in(\mathbf{Z}/(pq))^n} |\sigma(\mathbf{b})|^2 \\
= & \sum_{\mathbf{b}\in(\mathbf{Z}/(pq))^n} \sigma(\mathbf{b})\cdot\overline{\sigma(\mathbf{b})} \\
= & \sum_{0\le s,t\le T-1} \left(\sum_{b_0\in\mathbf{Z}/(pq)} e_{pq}\left(b_0\left(a(s)-a(t)\right)\right)\right)\cdot\cdots \\
& \qquad \cdot\left(\sum_{b_{n-1}\in\mathbf{Z}/(pq)} e_{pq}\left(b_{n-1}\left(a(s+n-1)-a(t+n-1)\right)\right)\right) \\
= & \sum_{\substack{0\le s,t\le T-1\\ s=t}} \left(\sum_{b_0\in\mathbf{Z}/(pq)} e_{pq}\left(b_0\left(a(s)-a(t)\right)\right)\right)\cdot\cdots \\
& \qquad \cdot\left(\sum_{b_{n-1}\in\mathbf{Z}/(pq)} e_{pq}\left(b_{n-1}\left(a(s+n-1)-a(t+n-1)\right)\right)\right) \qquad (9) \\
= & T\cdot(pq)^n, \qquad (10)
\end{aligned}$$

where the equality (9) holds since for $0\le s,t\le T-1$,

$$(a(s),\cdots a(s+n-1)) = (a(t),\cdots a(t+n-1)) \text{ if and only if } s=t.$$

Let $\mathbf{d}=(1,0,\cdots,0)\in(\mathbf{Z}/(pq))^n$ and $\Omega=\{\mathbf{d}\cdot A^t \mid 0\le t\le T-1\}$. By Lemma 5, we have $|\Omega|=T$. Thus, (5), (8) and (10) yield

$$\begin{aligned}
T\cdot\left|\sum_{t=0}^{T-1} e_{pq}(a(t))\right|^2 &= T\cdot|\sigma(\mathbf{d})|^2 \\
&= \sum_{t=0}^{T-1}\left|\sigma\left(\mathbf{d}A^t\right)\right|^2 \\
&= \sum_{\mathbf{b}\in\Omega}|\sigma(\mathbf{b})|^2 \\
&\le \sum_{\mathbf{b}\in(\mathbf{Z}/(pq))^n}|\sigma(\mathbf{b})|^2 \\
&= T\cdot(pq)^n,
\end{aligned}$$

and so we get

$$\left|\sum_{t=0}^{T-1} e_{pq}\left(a\left(t\right)\right)\right| \leq \left(pq\right)^{\frac{n}{2}}.$$

■

Lemma 7 *Let $\underline{a}$ be a primitive sequence generated by a primitive polynomial of degree $n \geq 2$ over $\mathbf{Z}/(pq)$ with period $T = \mathrm{lcm}\left(p^n - 1, q^n - 1\right)$. For any fixed elements $s_p \in \mathbf{Z}/(p)$ and $s_q \in \mathbf{Z}/(q)$, we have*

$$\sum_{t=0}^{T-1}\sum_{h_1=0}^{p-1} e_p\left(h_1\left(a\left(t\right) - s_p\right)\right) = \begin{cases} \frac{pT}{p^n-1}\left(p^{n-1}-1\right), & \text{if } s_p = 0; \\ \frac{pT}{p^n-1}p^{n-1}, & \text{if } s_p \in \mathbf{Z}/(p)^*. \end{cases} \tag{11}$$

and

$$\sum_{t=0}^{T-1}\sum_{h_2=0}^{q-1} e_q\left(h_2\left(a\left(t\right) - s_q\right)\right) = \begin{cases} \frac{qT}{q^n-1}\left(q^{n-1}-1\right), & \text{if } s_q = 0; \\ \frac{qT}{q^n-1}q^{n-1}, & \text{if } s_q \in \mathbf{Z}/(q)^*. \end{cases} \tag{12}$$

Proof. Let $\underline{b} = \left[\underline{a}\right]_{\mathrm{mod}\, p}$. Since $\underline{b}$ is a primitive sequence generated by $f(x)$ over $\mathbf{Z}/(p)$, it follows that

$$N\left(\underline{b}^T, s_p\right) = \frac{1}{p}\sum_{t=0}^{T-1}\sum_{h_1=0}^{p-1} e_p\left(h_1\left(b\left(t\right) - s_p\right)\right) = \frac{1}{p}\sum_{t=0}^{T-1}\sum_{h_1=0}^{p-1} e_p\left(h_1\left(a\left(t\right) - s_p\right)\right).$$

Hence, (11) immediately follows from the theory of m-sequence over finite fields. Similarly, we can get (12). ■

Let $\underline{a}$ and T be described as in Lemma 7. For any fixed element $s \in \mathbf{Z}/(pq)$, set $s_p = [s]_{\mathrm{mod}\, p}$ and $s_q = [s]_{\mathrm{mod}\, q}$. Then

$$\begin{aligned} N\left(\underline{a}^T, s\right) &= \frac{1}{pq}\sum_{t=0}^{T-1}\left(\sum_{h_1=0}^{p-1} e_p\left(h_1\left(a\left(t\right) - s_p\right)\right)\cdot\sum_{h_2=0}^{q-1} e_q\left(h_2\left(a\left(t\right) - s_q\right)\right)\right) \\ &= -\frac{T}{pq} + \frac{1}{pq}\sum_{t=0}^{T-1}\sum_{h_1=0}^{p-1} e_p\left(h_1\left(a\left(t\right) - s_p\right)\right) + \frac{1}{pq}\sum_{t=0}^{T-1}\sum_{h_2=0}^{q-1} e_q\left(h_2\left(a\left(t\right) - s_q\right)\right) \\ &\quad + \frac{1}{pq}\sum_{t=0}^{T-1}\sum_{h_1=1}^{p-1}\sum_{h_2=1}^{q-1} e_p\left(h_1\left(a\left(t\right) - s_p\right)\right) e_q\left(h_2\left(a\left(t\right) - s_q\right)\right). \end{aligned} \tag{13}$$

Denote

$$E\left(s_p, s_q\right) = -\frac{T}{pq} + \frac{1}{pq}\sum_{t=0}^{T-1}\sum_{h_1=0}^{p-1} e_p\left(h_1\left(a\left(t\right) - s_p\right)\right) + \frac{1}{pq}\sum_{t=0}^{T-1}\sum_{h_2=0}^{q-1} e_q\left(h_2\left(a\left(t\right) - s_q\right)\right). \quad (14)$$

Then by Lemma 7, we can deduce that

$$E\left(s_p, s_q\right) = \begin{cases} \frac{T}{pq}\left(1 - \frac{p-1}{p^n-1} - \frac{q-1}{q^n-1}\right), \text{ if } s_p = 0 \text{ and } s_q = 0; \\ \frac{T}{pq}\left(1 + \frac{1}{p^n-1} - \frac{q-1}{q^n-1}\right), \text{ if } s_p \in \mathbf{Z}/(p)^* \text{ and } s_q = 0; \\ \frac{T}{pq}\left(1 - \frac{p-1}{p^n-1} + \frac{1}{q^n-1}\right), \text{ if } s_p = 0 \text{ and } s_q \in \mathbf{Z}/(q)^*; \\ \frac{T}{pq}\left(1 + \frac{1}{p^n-1} + \frac{1}{q^n-1}\right), \text{ if } s_p \in \mathbf{Z}/(p)^* \text{ and } s_q \in \mathbf{Z}/(q)^*. \end{cases} \quad (15)$$

From (13) and (14) we can get

$$\begin{aligned} \left|N\left(\underline{a}^T, s\right) - E\left(s_p, s_q\right)\right| &= \frac{1}{pq}\left|\sum_{h_1=1}^{p-1}\sum_{h_2=1}^{q-1}\sum_{t=0}^{T-1} e_p\left(h_1\left(a\left(t\right) - s_p\right)\right) e_q\left(h_2\left(a\left(t\right) - s_q\right)\right)\right| \\ &\le \frac{1}{pq}\sum_{h_1=1}^{p-1}\sum_{h_2=1}^{q-1}\left|\sum_{t=0}^{T-1} e_p\left(h_1 a\left(t\right)\right) e_q\left(h_2 a\left(t\right)\right)\right| \\ &= \frac{1}{pq}\sum_{h_1=1}^{p-1}\sum_{h_2=1}^{q-1}\left|\sum_{t=0}^{T-1} e_{pq}\left(\left(qh_1 + ph_2\right) a\left(t\right)\right)\right| \\ &\le \frac{(p-1)\cdot(q-1)}{pq}\cdot(pq)^{\frac{n}{2}}. \end{aligned} \quad (16)$$

The last inequality (16) follows from Lemma 6 and the fact that $\left[\left(qh_1 + ph_2\right)\underline{a}\right]_{\mathrm{mod}\, pq}$ is also a primitive sequence over $\mathbf{Z}/(pq)$ for $1 \le h_1 \le p-1$ and $1 \le h_2 \le q-1$. Therefore, we have the following theorem.

Theorem 8 *Let $\underline{a}$ be a primitive sequence of order $n \ge 2$ over $\mathbf{Z}/(pq)$ with period $T = \mathrm{lcm}\left(p^n - 1, q^n - 1\right)$. For a given element $s \in \mathbf{Z}/(pq)$, the element s occurs in the sequence $\underline{a}$ if*

$$E\left(s_p, s_q\right) > \frac{(p-1)\cdot(q-1)}{pq}\cdot(pq)^{\frac{n}{2}},$$

where $s_p = [s]_{\mathrm{mod}\, p}$, $s_q = [s]_{\mathrm{mod}\, q}$ and $E\left(s_p, s_q\right)$ is defined in (15). In particular, every element in $\mathbf{Z}/(pq)$ occurs in the sequence $\underline{a}$ if

$$T\cdot\left(1 - \frac{p-1}{p^n-1} - \frac{q-1}{q^n-1}\right) > (p-1)\cdot(q-1)\cdot(pq)^{\frac{n}{2}}. \quad (17)$$

Proportion of (n, p, q) satisfying the inequality (17) of Theorem 8 is tested under different ranges of n, p and q, and the results are listed in Table 1, where $prime\,(k)$ is the k-th prime number. For example, the proportion is 96.461% for $2 \le n \le 31$ and $3 \le p < q \le prime\,(200) = 1223$. It can be seen from Table 1 that the proportion is very close to 100% if $n > 2$.

Table 1 Proportion of $_{(n,p,q)}$ satisfying the inequality (17) of Theorem 8

n	$3 \le p < q \le prime\,(k)$					
	$k = 200$	$k = 500$	$k = 1000$	$k = 3000$	$k = 5000$	$k = 10000$
$2 \le n \le 31$	96.461%	96.570%	96.612%	96.644%	96.562%	96.658%
$3 \le n \le 31$	99.787%	99.900%	99.944%	99.977%	99.985%	99.991%
$4 \le n \le 31$	99.921%	99.977%	99.991%	99.998%	99.999%	99.999%
$5 \le n \le 31$	100%	100%	100%	99.999%	99.999%	99.999%
$6 \le n \le 31$	100%	100%	100%	99.999%	99.999%	99.999%
$7 \le n \le 31$	100%	100%	100%	100%	100%	100%

Remark 9 *Not all elements in* $\mathbf{Z}/(pq)$ *occur in a primitive sequence of order* $n = 2$ *over* $\mathbf{Z}/(pq)$. *For example,* $f(x) = x^2 - (4x + 13)$ *is a primitive polynomial of degree* $n = 2$ *over* $\mathbf{Z}/(pq)$ *with period* $T = \mathrm{lcm}\,(3^2 - 1, 5^2 - 1) = 24$ *and*

$$\underline{a} = (1, 0, 13, 7, 2, 9, 2, 5, 1, 9, 4, 13, 14, 0, 2, 8, 13, 6, 13, 10, 14, 6, 11, 2, \cdots)$$

is a primitive sequence generated by $f(x)$ *over* $\mathbf{Z}/(pq)$. *It can be seen that the element* 3 *and the element* 12 *do not occur in the sequence* $\underline{a}$.

Corollary 10 *Let* $\underline{a}$ *and* T *be given as in Theorem 8. For* $n > 2$, *every element in* $\mathbf{Z}/(pq)$ *occurs in the sequence* $\underline{a}$ *if*

$$q \ge \left(\frac{403}{354}\right)^{\frac{2}{n-2}} \cdot p^{\frac{n+2}{n-2}}.$$

Proof. On the one hand, we have

$$\begin{aligned} & T\cdot\left(1-\frac{p-1}{p^n-1}-\frac{q-1}{q^n-1}\right) \\ = \;& T\cdot\left(1-\frac{1}{p^{n-1}+\cdots+p+1}-\frac{1}{q^{n-1}+\cdots+q+1}\right) \\ \geq \;& T\cdot\left(1-\frac{1}{p^2+p+1}-\frac{1}{q^2+q+1}\right) \\ \geq \;& T\cdot\left(1-\frac{1}{3^2+3+1}-\frac{1}{5^2+5+1}\right) \\ = \;& \frac{359}{403}\cdot T \\ \geq \;& \frac{359}{403}\cdot(q^n-1)\,. \end{aligned} \tag{18}$$

Note that $q^n \geq 5^3 = 125$, and so it follows from (18) that

$$T\cdot\left(1-\frac{p-1}{p^n-1}-\frac{q-1}{q^n-1}\right) \geq \frac{359}{403}\cdot(q^n-1) > \frac{354}{403}\cdot q^n.$$

On the other hand, it is clear that

$$(p-1)\cdot(q-1)\cdot(pq)^{\frac{n}{2}} < (pq)^{\frac{n}{2}+1}\,. \tag{19}$$

Since $q \geq \left(\frac{403}{354}\right)^{\frac{2}{n-2}}\cdot p^{\frac{n+2}{n-2}}$, we get

$$\frac{\frac{354}{403}\cdot q^n}{(pq)^{\frac{n}{2}+1}} = \frac{\frac{354}{403}\cdot q^{\frac{n}{2}-1}}{p^{\frac{n}{2}+1}} \geq 1. \tag{20}$$

Then (18), (19) and (20) yield

$$\begin{aligned} T\cdot\left(1-\frac{p-1}{p^n-1}-\frac{q-1}{q^n-1}\right) \;&>\; \frac{354}{403}\cdot q^n \\ &\geq\; (pq)^{\frac{n}{2}+1} \\ &>\; (p-1)\cdot(q-1)\cdot(pq)^{\frac{n}{2}}\,, \end{aligned}$$

and so the corollary follows from Theorem 8. ■

For two given odd prime numbers p and q with $p < q$, since

$$\lim_{n\to\infty}\left(\frac{403}{354}\right)^{\frac{2}{n-2}}\cdot p^{\frac{n+2}{n-2}} = p,$$

there exists a positive integer N such that $q \geq \left(\frac{403}{354}\right)^{\frac{2}{n-2}} \cdot p^{\frac{n+2}{n-2}}$ for any integer $n > N$, and so it follows from Corollary 10 that every element in $\mathbf{Z}/(pq)$ occurs in a primitive sequence $\underline{a}$ of order n.

3 Distinctness of primitive sequences over $\mathbf{Z}/(pq)$ modulo 2

In this section, we first give the complete proof of Theorem 3 presented in Section 1 and then discuss the proportion of primitive sequences covered by Theorem 3.

3.1 The proof of Theorem 3

Throughout this subsection, let p and q be two odd prime numbers with $p < q$ and $f(x)$ be a primitive polynomial of degree $n \geq 2$ over $\mathbf{Z}/(pq)$.

Lemma 11 *Let $\underline{a}$ and $\underline{b}$ be two sequences in $G'(f(x), pq)$ with $[\underline{a}]_{\mathrm{mod}\,2} = [\underline{b}]_{\mathrm{mod}\,2}$. If*

(1) *there exist a positive integer S and an even number C in $\mathbf{Z}/(pq)$ such that $x^S - C \equiv 0 \,(\mathrm{mod}\, f(x), pq)$; and*

(2) *for any sequence $\underline{z} \in G'(f(x), pq)$, either 1 or $pq-1$ occurs in $\underline{z}$,*

then $[\underline{a}]_{\mathrm{mod}\,p} = [\underline{b}]_{\mathrm{mod}\,p}$ or $[\underline{a}]_{\mathrm{mod}\,q} = [\underline{b}]_{\mathrm{mod}\,q}$.

Proof. Denote $\underline{c} = [\underline{a} - \underline{b}]_{\mathrm{mod}\,pq}$. It suffices to prove that $[\underline{c}]_{\mathrm{mod}\,p} = \underline{0}$ or $[\underline{c}]_{\mathrm{mod}\,q} = \underline{0}$.

Suppose $[\underline{c}]_{\mathrm{mod}\,p} \neq \underline{0}$ and $[\underline{c}]_{\mathrm{mod}\,q} \neq \underline{0}$. Then $\underline{c} \in G'(f(x), pq)$, and so it follows from condition (2) that there exists an integer $t \geq 0$ such that $c\,(t) = 1$ or $c\,(t) = pq - 1$.

If $c\,(t) = 1$, i.e., $[a(t) - b(t)]_{\mathrm{mod}\,pq} = 1$, then it follows from $[a\,(t)]_{\mathrm{mod}\,2} = [b\,(t)]_{\mathrm{mod}\,2}$ that

$$a\,(t) = 0 \text{ and } b\,(t) = pq - 1.$$

Thus, by condition (1) we have

$$a\,(t+S) = [C \cdot 0]_{\bmod pq} = 0 \text{ and } b\,(t+S) = [C \cdot (pq-1)]_{\bmod pq} = pq - C.$$

Note that C is an even number, and so this implies that

$$[a\,(t+S)]_{\bmod 2} = 0 \neq 1 = [pq - C]_{\bmod 2} = [b\,(t+S)]_{\bmod 2}\,,$$

a contradiction to the assumption that $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$.

Similarly, it can be shown that if $c\,(t) = pq - 1$, then $[\underline{a}]_{\bmod 2} \neq [\underline{b}]_{\bmod 2}$.

Therefore, we get that either $[\underline{c}]_{\bmod p} = \underline{0}$ or $[\underline{c}]_{\bmod q} = \underline{0}$. ■

In the following we discuss the two cases $[\underline{a}]_{\bmod p} = [\underline{b}]_{\bmod p}$ and $[\underline{a}]_{\bmod q} = [\underline{b}]_{\bmod q}$, respectively.

Lemma 12 *Let $\underline{a}$ and $\underline{b}$ be two sequences in $G'(f(x), pq)$ with $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$ and $[\underline{a}]_{\bmod p} = [\underline{b}]_{\bmod p}$. Then $\underline{a} = \underline{b}$ if for any sequence $\underline{z} \in G'(f(x), pq)$, every element in $\mathbf{Z}/(pq)$ occurs in $\underline{z}$.*

Proof. Since $[\underline{a}]_{\bmod p} = [\underline{b}]_{\bmod p}$, it suffices to show $[\underline{a}]_{\bmod q} = [\underline{b}]_{\bmod q}$. By the Chinese Remainder Theorem we get that

$$\underline{a} \equiv q \cdot \left[q^{-1} \cdot \underline{a}\right]_{\bmod p} + p \cdot \left[p^{-1} \cdot \underline{a}\right]_{\bmod q} \bmod pq \tag{21}$$

and

$$\underline{b} \equiv q \cdot \left[q^{-1} \cdot \underline{b}\right]_{\bmod p} + p \cdot \left[p^{-1} \cdot \underline{b}\right]_{\bmod q} \bmod pq. \tag{22}$$

Denote $\underline{m}_1 = [q^{-1} \cdot \underline{a}]_{\bmod p} = [q^{-1} \cdot \underline{b}]_{\bmod p}$, $\underline{m}_2 = [p^{-1} \cdot \underline{a}]_{\bmod q}$ and $\underline{m}_3 = [p^{-1} \cdot \underline{b}]_{\bmod q}$. It can be seen that $\underline{m}_1 \in G'(f(x), p)$, $\underline{m}_2, \underline{m}_3 \in G'(f(x), q)$, and (21), (22) can be written as

$$\underline{a} = [q \cdot \underline{m}_1 + p \cdot \underline{m}_2]_{\bmod pq} \text{ and } \underline{b} = [q \cdot \underline{m}_1 + p \cdot \underline{m}_3]_{\bmod pq}\,. \tag{23}$$

Suppose $\underline{m}_2 \neq \underline{m}_3$. We will show $[\underline{a}]_{\bmod 2} \neq [\underline{b}]_{\bmod 2}$ by discussing the following two cases, respectively.

Case 1: $\underline{m}_2$ and $\underline{m}_3$ are linearly independent over $\mathbf{Z}/(q)$

Since $\underline{m}_2$ and $\underline{m}_3$ are two m-sequences over the finite field $\mathbf{Z}/(q)$, it can be seen that there exists an integer $t \geq 0$ such that $m_2(t) = 0$ and $m_3(t) = 1$. Hence (23) yields

$$a(t) = [q \cdot m_1(t)]_{\mathrm{mod}\, pq} \text{ and } b(t) = [q \cdot m_1(t) + p]_{\mathrm{mod}\, pq}. \tag{24}$$

Note that $q \cdot m_1(t) \leq q \cdot (p-1) < pq$ and $q \cdot m_1(t) + p \leq q \cdot (p-1) + p < pq$, and so (24) implies that

$$a(t) = q \cdot m_1(t) \text{ and } b(t) = q \cdot m_1(t) + p.$$

This shows that $[a(t)]_{\mathrm{mod}\, 2} \neq [b(t)]_{\mathrm{mod}\, 2}$.

Case 2: $\underline{m}_2$ and $\underline{m}_3$ are linearly dependent over $\mathbf{Z}/(q)$

Since $\underline{m}_2 \neq \underline{m}_3$, we have $\underline{m}_3 = [\lambda \cdot \underline{m}_2]_{\mathrm{mod}\, q}$ for some integer $2 \leq \lambda \leq q-1$. It follows from condition (1) that $(m_1(t), m_2(t))$ runs through the set $\{(u, v) \mid u \in \mathbf{Z}/(p), v \in \mathbf{Z}/(q)\}$ when t runs from 0 to $\mathrm{lcm}(p^n - 1, q^n - 1) - 1$.

If λ is even, then choose an integer $t \geq 0$ such that $m_1(t) = 0$ and $m_2(t) = 1$, and so (23) immediately yields

$$a(t) = p \text{ and } b(t) = \lambda \cdot p < pq.$$

This shows that $[a(t)]_{\mathrm{mod}\, 2} \neq [b(t)]_{\mathrm{mod}\, 2}$.

If λ is odd, then let us denote $\delta = \left\lceil \frac{q}{\lambda} \right\rceil$. Since

$$q = \lambda \cdot \frac{q}{\lambda} \leq \lambda \cdot \delta = \lambda \cdot \left\lceil \frac{q}{\lambda} \right\rceil < \lambda \cdot \left(\frac{q}{\lambda} + 1 \right) = q + \lambda < 2 \cdot q,$$

it follows that $[\lambda \cdot \delta]_{\mathrm{mod}\, q} = \lambda \cdot \delta - q$. Choose an integer $t \geq 0$ such that $m_1(t) = 0$ and $m_2(t) = \delta$. Then (23) yields

$$a(t) = [p \cdot \delta]_{\mathrm{mod}\, pq} = p \cdot \delta$$

and

$$b(t) = \left[p \cdot [\lambda \cdot \delta]_{\mathrm{mod}\, q} \right]_{\mathrm{mod}\, pq} = p \cdot [\lambda \cdot \delta]_{\mathrm{mod}\, q} = p \cdot (\lambda \cdot \delta - q).$$

It follows that

$$[a(t)]_{\mathrm{mod}\,2} = [\delta]_{\mathrm{mod}\,2} \neq [\delta - 1]_{\mathrm{mod}\,2} = [p \cdot (\lambda \cdot \delta - q)]_{\mathrm{mod}\,2} = [b(t)]_{\mathrm{mod}\,2}.$$

The above discussions imply that $\underline{m}_2 = \underline{m}_3$, and so $[\underline{a}]_{\mathrm{mod}\,q} = [\underline{b}]_{\mathrm{mod}\,q}$. ■

For a positive integer u, let $v_2(u)$ denote the greatest nonnegative integer m such that 2^m divides u. With the notation, $v_2(u) = 0$ if and only if u is odd.

Lemma 13 *Let $\underline{a}$ and $\underline{b}$ be two sequences in $G'(f(x), pq)$ with $[\underline{a}]_{\mathrm{mod}\,2} = [\underline{b}]_{\mathrm{mod}\,2}$ and $[\underline{a}]_{\mathrm{mod}\,q} = [\underline{b}]_{\mathrm{mod}\,q}$. Set $T = \mathrm{lcm}(p^n - 1, q^n - 1)$ and*

$$E = \begin{cases} 0, & \text{if } v_2(p^n - 1) \neq v_2(q^n - 1); \\ \left\lfloor \frac{q}{p} \right\rfloor \cdot \mathrm{lcm}\left(p^n - 1, \frac{q^n - 1}{q - 1}\right), & \text{if } v_2(p^n - 1) = v_2(q^n - 1). \end{cases}$$

Then $\underline{a} = \underline{b}$ if

(1) *for any sequence $\underline{z} \in G'(f(x), pq)$, every element in $\mathbf{Z}/(pq)$ occurs in $\underline{z}$; and*

(2) *$T > E$.*

Proof. Since $[\underline{a}]_{\mathrm{mod}\,q} = [\underline{b}]_{\mathrm{mod}\,q}$, it suffices to show $[\underline{a}]_{\mathrm{mod}\,p} = [\underline{b}]_{\mathrm{mod}\,p}$. Proceed as in the proof of Lemma 12, we get

$$\underline{a} = [q \cdot \underline{m}_1 + p \cdot \underline{m}_3]_{\mathrm{mod}\,pq} \text{ and } \underline{b} = [q \cdot \underline{m}_2 + p \cdot \underline{m}_3]_{\mathrm{mod}\,pq}, \tag{25}$$

where $\underline{m}_1 = [q^{-1} \cdot \underline{a}]_{\mathrm{mod}\,p}, \underline{m}_2 = [q^{-1} \cdot \underline{b}]_{\mathrm{mod}\,p} \in G'(f(x), p)$ and $\underline{m}_3 = [p^{-1} \cdot \underline{a}]_{\mathrm{mod}\,q} = [p^{-1} \cdot \underline{b}]_{\mathrm{mod}\,q} \in G'(f(x), q)$.

Suppose $\underline{m}_1 \neq \underline{m}_2$. We will show $[\underline{a}]_{\mathrm{mod}\,2} \neq [\underline{b}]_{\mathrm{mod}\,2}$ or $T \leq E$ by discussing the following two cases, respectively.

Case 1: $\underline{m}_1$ and $\underline{m}_2$ are linearly independent over $\mathbf{Z}/(p)$

Since $\underline{m}_1$ and $\underline{m}_2$ are two m-sequences over the finite field $\mathbf{Z}/(p)$, there exists an integer $t \geq 0$ such that $m_1(t) = 0$ and $m_2(t) = 1$. Let $q = k \cdot p + r$ with $0 < r \leq p - 1$.

Case 1.1: $0 \leq m_3(t) \leq q-k-1$

Since $q \cdot 1 + p \cdot m_3(t) \leq q + p \cdot (q-k-1) < pq$, we have

$$a(t) = [0 + p \cdot m_3(t)]_{\bmod pq} = p \cdot m_3(t)$$

and

$$b(t) = [q \cdot 1 + p \cdot m_3(t)]_{\bmod pq} = q + p \cdot m_3(t),$$

then we get $[a(t)]_{\bmod 2} = [m_3(t)]_{\bmod 2} \neq [m_3(t)+1]_{\bmod 2} = [b(t)]_{\bmod 2}$.

Case 1.2: $q-k \leq m_3(t) \leq q-1$

(a) If $v_2(p^n-1) > v_2(q^n-1)$, then we get

$$\left[\frac{T}{2}\right]_{\bmod p^n-1} = \frac{p^n-1}{2} \text{ and } \left[\frac{T}{2}\right]_{\bmod q^n-1} = 0. \tag{26}$$

Note that $f(x) \pmod p$ is a primitive polynomial over $\mathbf{Z}/(p)$ with $per(f(x), p) = p^n - 1$, and so $x^{\frac{p^n-1}{2}} \equiv -1 \bmod (f(x), p)$. Then (26) implies that

$$x^{\frac{T}{2}} \equiv x^{\frac{p^n-1}{2}} \equiv -1 \bmod (f(x), p) \text{ and } x^{\frac{T}{2}} \equiv 1 \bmod (f(x), q).$$

Applying $x^{\frac{T}{2}} \equiv -1 \bmod (f(x), p)$ to $\underline{m}_1$, $\underline{m}_2$ and using $m_1(t) = 0$, $m_2(t) = 1$, we obtain

$$m_1\left(t + \frac{T}{2}\right) = [-m_1(t)]_{\bmod p} = 0, m_2\left(t + \frac{T}{2}\right) = [-m_2(t)]_{\bmod p} = p-1. \tag{27}$$

Applying $x^{\frac{T}{2}} \equiv 1 \bmod (f(x), q)$ to $\underline{m}_3$ leads to

$$m_3\left(t + \frac{T}{2}\right) = m_3(t). \tag{28}$$

Thus (25), (27) and (28) yield

$$a\left(t + \frac{T}{2}\right) = \left[q \cdot m_1\left(t + \frac{T}{2}\right) + p \cdot m_3\left(t + \frac{T}{2}\right)\right]_{\bmod pq} = p \cdot m_3(t)$$

and

$$b\left(t + \frac{T}{2}\right) = \left[q \cdot m_2\left(t + \frac{T}{2}\right) + p \cdot m_3\left(t + \frac{T}{2}\right)\right]_{\bmod pq} = [q \cdot (p-1) + p \cdot m_3(t)]_{\bmod pq}.$$

Since $q-k \leq m_3(t) \leq q-1$, it follows that

$$q \cdot (p-1) + p \cdot m_3(t) \geq pq + p \cdot (q-k) - q > pq + (p-2) \cdot q > pq$$

and

$$q \cdot (p-1) + p \cdot m_3(t) \leq pq + p \cdot (q-1) - q < 2pq,$$

and so

$$b\left(t + \frac{T}{2}\right) = \left[q \cdot (p-1) + p \cdot m_3(t)\right]_{\bmod pq} = p \cdot m_3(t) - q.$$

Hence we have

$$\left[a\left(t + \frac{T}{2}\right)\right]_{\bmod 2} = \left[m_3(t)\right]_{\bmod 2} \neq \left[m_3(t) - 1\right]_{\bmod 2} = \left[b\left(t + \frac{T}{2}\right)\right]_{\bmod 2}.$$

(b) If $v_2(p^n - 1) < v_2(q^n - 1)$, then we get

$$\left[\frac{T}{2}\right]_{\bmod p^n - 1} = 0 \text{ and } \left[\frac{T}{2}\right]_{\bmod q^n - 1} = \frac{q^n - 1}{2},$$

and so

$$x^{\frac{T}{2}} \equiv 1 \bmod (f(x), p) \text{ and } x^{\frac{T}{2}} \equiv x^{\frac{q^n - 1}{2}} \equiv -1 \bmod (f(x), q).$$

Similarly, we can get

$$m_1\left(t + \frac{T}{2}\right) = m_1(t) = 0, m_2\left(t + \frac{T}{2}\right) = m_2(t) = 1.$$

and

$$m_3\left(t + \frac{T}{2}\right) = \left[-m_3(t)\right]_{\bmod q} = q - m_3(t).$$

Hence

$$a\left(t + \frac{T}{2}\right) = \left[q \cdot m_1\left(t + \frac{T}{2}\right) + p \cdot m_3\left(t + \frac{T}{2}\right)\right]_{\bmod pq} = p \cdot (q - m_3(t))$$

and

$$b\left(t + \frac{T}{2}\right) = \left[q \cdot m_2\left(t + \frac{T}{2}\right) + p \cdot m_3\left(t + \frac{T}{2}\right)\right]_{\bmod pq} = \left[q + p \cdot (q - m_3(t))\right]_{\bmod pq}. \tag{29}$$

Since $q+p \le q+p\cdot(q-m_3(t)) \le q+kp < 2q < pq$, then (29) yields

$$b\left(t+\frac{T}{2}\right) = q+p\cdot(q-m_3(t)).$$

Therefore

$$\left[a\left(t+\frac{T}{2}\right)\right]_{\bmod 2} = [1-m_3(t)]_{\bmod 2} \neq [-m_3(t)]_{\bmod 2} = \left[b\left(t+\frac{T}{2}\right)\right]_{\bmod 2}.$$

(c) If $v_2(p^n-1) = v_2(q^n-1)$, then note that $\left\lfloor \frac{q}{p} \right\rfloor \ge 1$, and so by condition (2) we get

$$T > \operatorname{lcm}\left(p^n-1, \frac{q^n-1}{q-1}\right). \tag{30}$$

Since $f(x) \pmod q$ is a primitive polynomial of degree n over $\mathbf{Z}/(q)$, there exists a primitive element ξ in $\mathbf{Z}/(q)$ such that

$$x^{\frac{q^n-1}{q-1}} \equiv \xi \bmod (f(x), q).$$

Denote $S = \operatorname{lcm}\left(p^n-1, \frac{q^n-1}{q-1}\right)$. Then we get

$$x^S \equiv 1 \bmod (f(x), p) \text{ and } x^S \equiv \xi^h \bmod (f(x), q), \tag{31}$$

where $h = \left[\frac{S}{\frac{q^n-1}{q-1}}\right]_{\bmod q-1} = \left[\frac{(q-1)\cdot S}{q^n-1}\right]_{\bmod q-1} \neq 0$ (Otherwise $h=0$, and (31) yields $x^S \equiv 1 \bmod (f(x), pq)$, then (30) implies that $f(x)$ is not a primitive polynomial over $\mathbf{Z}/(pq)$, a contradiction). It follows from (25) and (31) that

$$\begin{aligned} a(t+k\cdot S) &= [q\cdot m_1(t+k\cdot S) + p\cdot m_3(t+k\cdot S)]_{\bmod pq} \\ &= \left[q\cdot m_1(t) + p\cdot \xi^{hk}\cdot m_3(t)\right]_{\bmod pq} \\ &= p\cdot\left[\xi^{hk}\cdot m_3(t)\right]_{\bmod q} \end{aligned} \tag{32}$$

and

$$\begin{aligned} b(t+k\cdot S) &= [q\cdot m_2(t+k\cdot S) + p\cdot m_3(t+k\cdot S)]_{\bmod pq} \\ &= \left[q\cdot m_2(t) + p\cdot \xi^{hk}\cdot m_3(t)\right]_{\bmod pq} \\ &= \left[q+p\cdot\left[\xi^{hk}\cdot m_3(t)\right]_{\bmod q}\right]_{\bmod pq}, \end{aligned} \tag{33}$$

for $0 \leq k < \frac{T}{S}$. In the following we will deduce a contradiction by showing that $T \leq E$.

First, we claim that $\left[\xi^{hk_1} \cdot m_3(t)\right]_{\bmod q} \neq \left[\xi^{hk_2} \cdot m_3(t)\right]_{\bmod q}$ if $k_1 \neq k_2$ for $0 \leq k_1, k_2 < \frac{T}{S}$. Otherwise, there exist two integer k_1 and k_2, $0 \leq k_1 < k_2 < \frac{T}{S}$ such that $\left[\xi^{hk_1} \cdot m_3(t)\right]_{\bmod q} = \left[\xi^{hk_2} \cdot m_3(t)\right]_{\bmod q}$. Then we get $\left[\xi^{h(k_2-k_1)}\right]_{\bmod q} = 1$. Using $x^S \equiv \xi^h \bmod (f(x), q)$, it follows that

$$x^{S\cdot(k_2-k_1)} \equiv 1 \bmod (f(x), q),$$

where $S \cdot (k_2 - k_1) < T$, a contradiction to the assumption that $f(x)$ is a primitive polynomial over $\mathbf{Z}/(pq)$.

Second, $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$ implies that $[a(t + k \cdot S)]_{\bmod 2} = [b(t + k \cdot S)]_{\bmod 2}$ for $0 \leq k < \frac{T}{S}$, then it follows from (32) and (33) that

$$q + p \cdot \left[\xi^{hk} \cdot m_3(t)\right]_{\bmod q} \geq pq \text{ for } 0 \leq k < \frac{T}{S}.$$

Note that $\left[\xi^{hk} \cdot m_3(t)\right]_{\bmod q}$ is an integer, and so we can get

$$q - \left\lfloor \frac{q}{p} \right\rfloor \leq \left[\xi^{hk} \cdot m_3(t)\right]_{\bmod q} \leq q - 1 \text{ for } 0 \leq k < \frac{T}{S}.$$

Hence we deduce $\frac{T}{S} \leq \left\lfloor \frac{q}{p} \right\rfloor$, i.e., $T \leq E$.

Case 2: $\underline{m}_1$ and $\underline{m}_2$ are linearly dependent over $\mathbf{Z}/(p)$

Since $\underline{m}_1 \neq \underline{m}_2$, we have $\underline{m}_2 = [\lambda \cdot \underline{m}_1]_{\bmod p}$ for some integer $2 \leq \lambda \leq p - 1$. It follows from condition (1) that $(m_1(t), m_2(t))$ runs through the set $\{(u, v) \mid u \in \mathbf{Z}/(p), v \in \mathbf{Z}/(q)\}$ when t runs from 0 to $T - 1$.

If λ is even, then choose an integer $t \geq 0$ such that $m_1(t) = 0$ and $m_3(t) = 1$, and so

$$a(t) = q \text{ and } b(t) = \lambda \cdot p < pq.$$

This shows that $[a(t)]_{\bmod 2} = 1 \neq 0 = [b(t)]_{\bmod 2}$.

If λ is odd, then let us denote $\delta = \left\lceil \frac{p}{\lambda} \right\rceil$. Since

$$p = \lambda \cdot \frac{p}{\lambda} \leq \lambda \cdot \delta = \lambda \cdot \left\lceil \frac{p}{\lambda} \right\rceil < \lambda \cdot \left(\frac{p}{\lambda} + 1\right) = p + \lambda < 2 \cdot p,$$

it follows that $[\lambda \cdot \delta]_{\bmod p} = \lambda \cdot \delta - p$. Choose an integer $t \geq 0$ such that $m_1(t) = \delta$ and $m_3(t) = 0$, then we have

$$a(t) = [q \cdot \delta]_{\bmod pq} = q \cdot \delta$$

and

$$b(t) = \left[q \cdot [\lambda \cdot \delta]_{\bmod q}\right]_{\bmod pq} = q \cdot [\lambda \cdot \delta]_{\bmod p} = q \cdot (\lambda \cdot \delta - p).$$

It follows that

$$[a(t)]_{\bmod 2} = [\delta]_{\bmod 2} \neq [\delta - 1]_{\bmod 2} = [q \cdot (\lambda \cdot \delta - p)]_{\bmod 2} = [b(t)]_{\bmod 2}.$$

The above discussions imply that $\underline{m}_1 = \underline{m}_2$, and so $[\underline{a}]_{\bmod p} = [\underline{b}]_{\bmod p}$. ■

Proof of Theorem 3. It can be seen that Theorem 3 immediately follows from Theorem 8, Lemma 11, Lemma 12 and Lemma 13. ■

3.2 Discussions on the conditions of Theorem 3

Experiments show that the condition (2) of Theorem 3 is very weak. For example, the proportion of (n, p, q) satisfying it reaches 99.843% for $3 \leq n \leq 20$ and $3 \leq p < q \leq 104729$, where 104729 is the 10000-th prime number. Therefore, in this subsection we focus on the condition (1) of Theorem 3.

Let p and q be two odd prime numbers and let Ω_p and Ω_q be the set of primitive elements in $\mathbf{Z}/(p)$ and the set of primitive elements in $\mathbf{Z}/(q)$, respectively. If $f(x)$ is a primitive polynomial over $\mathbf{Z}/(pq)$ of degree $n \geq 2$, then $f(x)$ is a primitive polynomial both over $\mathbf{Z}/(p)$ and $\mathbf{Z}/(q)$. It follows that there exist a primitive element $\xi_p \in \Omega_p$ and a primitive element $\xi_q \in \Omega_q$ such that

$$x^{\frac{p^n-1}{p-1}} \equiv \xi_p \bmod (f(x), p) \text{ and } x^{\frac{q^n-1}{q-1}} \equiv \xi_q \bmod (f(x), q).$$

Let us denote

$$\theta_{p,n} = \frac{\operatorname{lcm}(\frac{p^n-1}{p-1}, \frac{q^n-1}{q-1})}{\frac{p^n-1}{p-1}} \text{ and } \theta_{q,n} = \frac{\operatorname{lcm}(\frac{p^n-1}{p-1}, \frac{q^n-1}{q-1})}{\frac{q^n-1}{q-1}}.$$

Then for any positive integer k we have

$$\begin{aligned} x^{k\cdot \mathrm{lcm}(\frac{p^n-1}{p-1},\frac{q^n-1}{q-1})} &\equiv \xi_p^{k\cdot\theta_{p,n}} \bmod (f(x), p), \\ x^{k\cdot \mathrm{lcm}(\frac{p^n-1}{p-1},\frac{q^n-1}{q-1})} &\equiv \xi_q^{k\cdot\theta_{q,n}} \bmod (f(x), q), \end{aligned}$$

and so

$$x^{k\cdot \mathrm{lcm}(\frac{p^n-1}{p-1},\frac{q^n-1}{q-1})} \equiv \mathrm{Lift}(\xi_p^{k\cdot\theta_{p,n}}, \xi_q^{k\cdot\theta_{q,n}}) \bmod (f(x), pq)$$

where $\mathrm{Lift}(\xi_p^{k\cdot\theta_{p,n}}, \xi_q^{k\cdot\theta_{q,n}})$ denotes the unique integer m between 0 and $pq-1$ such that

$$m \equiv \xi_p^{k\cdot\theta_{p,n}} \bmod p \quad \text{and} \quad m \equiv \xi_q^{k\cdot\theta_{q,n}} \bmod q.$$

This shows that if there exists some positive integer k such that $\mathrm{Lift}(\xi_p^{k\cdot\theta_{p,n}}, \xi_q^{k\cdot\theta_{q,n}})$ is an even number, then $f(x)$ satisfies the condition (1) of Theorem 3. Thus, if for every pair of primitive elements $(\xi_p, \xi_q) \in \Omega_p \times \Omega_q$, there is an integer k such that $\mathrm{Lift}(\xi_p^{k\cdot\theta_{p,n}}, \xi_q^{k\cdot\theta_{q,n}})$ is an even number, then every primitive polynomial over $\mathbf{Z}/(pq)$ of degree n satisfies the condition (1) of Theorem 3. Based on this observation, We tested the proportion of (n, p, q) satisfying the conditions of Theorem 3 for degree n up to 31 and odd prime numbers p, q up to the 168-th prime, and to make a comparison with the result of [18], we also tested the proportion of (n, p, q) satisfying the conditions of Theorem 1 in [18] for the same range of n and odd prime numbers p, q. Results are listed in Table 2. It can be seen from Table 2 that the sufficient conditions of our Theorem 3 are much weaker than those of Theorem 1 in [18].

Table 2 Comparison between the proportion of (n, p, q) satisfying the conditions of Theorem 3 and those of Theorem 1 in [18]

n	Theorem 3			Theorem 1 in [18]		
	$3 \le p < q \le prime(k)$			$3 \le p < q \le prime(k)$		
	$k = 50$	$k = 100$	$k = 168$	$k = 50$	$k = 100$	$k = 168$
$2 \le n \le 31$	$\ge 90.439\%$	$\ge 92.606\%$	$\ge 93.756\%$	46.638%	48.143%	48.765%
$3 \le n \le 31$	$\ge 93.558\%$	$\ge 95.800\%$	$\ge 96.989\%$	47.930%	49.434%	50.037%
$4 \le n \le 31$	$\ge 93.732\%$	$\ge 95.899\%$	$\ge 97.051\%$	46.747%	48.243%	48.858%
$5 \le n \le 31$	$\ge 94.174\%$	$\ge 96.121\%$	$\ge 97.184\%$	48.246%	49.767%	50.376%
$6 \le n \le 31$	$\ge 93.972\%$	$\ge 95.992\%$	$\ge 97.094\%$	46.775%	48.281%	48.914%
$7 \le n \le 31$	$\ge 94.153\%$	$\ge 96.095\%$	$\ge 97.168\%$	48.381%	49.920%	50.550%

Remark 14 *There do exist (n, p, q) that does not satisfy the condition (1) of Theorem 3. For example, $f(x) = x^4 + 4x^3 + 2x^2 + 3x + 3$ is a primitive polynomial over $\mathbf{Z}/(7 \times 101)$, and it can be verified that*

$$x^{k\cdot \mathrm{lcm}(\frac{7^n-1}{7-1}, \frac{11^n-1}{11-1})} \equiv \begin{cases} 405 \bmod (f(x), 7 \times 101), \text{ if } [k]_{\bmod 2} = 1; \\ 1 \bmod (f(x), 7 \times 101), \text{ if } [k]_{\bmod 2} = 0. \end{cases}$$

Therefore, there is no positive integer S and even number C in $\mathbf{Z}/(pq)$ such that $x^S - C \equiv 0 \pmod{f(x), pq}$.

It can be seen that for relatively larger prime numbers p, q, it is difficult for us to run through $\Omega_p \times \Omega_q$. Thus, in the following, we give another sufficient condition for (n, p, q) satisfying the condition (1) of Theorem 3, which is much easier to verify but stronger than the previous one discussed above. First, we introduce a classic result given by H. L. Garner in 1958.

Lemma 15 *([19])Let $m_1, m_2, \cdots, m_k$ be pairwise coprime positive integers. Then*

$$u = v_k \cdot m_{k-1} \cdots m_2 \cdot m_1 + \cdots + v_3 \cdot m_2 \cdot m_1 + v_2 \cdot m_1 + v_1$$

is a number satisfying

$$0 \le u < \prod_{i=1}^{k} m_i,\ u \equiv u_j \,(\mathrm{mod}\, m_j)\ \ for\ 1 \le j \le k,$$

where

$$\begin{aligned} v_1 &= [u_1]_{\mathrm{mod}\, m_1}, \\ v_2 &= [(u_2 - v_1)\cdot c_{1,2}]_{\mathrm{mod}\, m_2}, \\ v_3 &= [((u_3 - v_1)\cdot c_{1,3} - v_2)\cdot c_{2,3}]_{\mathrm{mod}\, m_3}, \\ &\cdots\cdots \\ v_k &= [(\cdots((u_k - v_1)\cdot c_{1,k} - v_2)\cdot c_{2,k} - \cdots - v_{k-1})\cdot c_{k-1,k}]_{\mathrm{mod}\, m_k}, \end{aligned}$$

with $c_{i,j} = \left[m_i^{-1}\right]_{\mathrm{mod}\, m_j}$, $1 \le i < j \le k$.

Based on Lemma 15, we are easy to get the following results.

Lemma 16 *Let p and q be two odd prime numbers and let $f(x)$ be a primitive polynomial of degree $n \ge 2$ over $\mathbf{Z}/(pq)$. Then there exist a positive integer S and an even number C in $\mathbf{Z}/(pq)$ such that*

$$x^S - C \equiv 0 \,\mathrm{mod}(f(x), pq),$$

if one of the following three conditions is satisfied:

(1) $v_2(p^n - 1) = v_2(q^n - 1)$;

(2) $v_2(p^n - 1) > v_2(q^n - 1)$ *and* $[p^{-1}]_{\mathrm{mod}\, q} > \frac{q}{2}$;

(3) $v_2(p^n - 1) < v_2(q^n - 1)$ *and* $[q^{-1}]_{\mathrm{mod}\, p} > \frac{p}{2}$.

Proof. Denote $T = \mathrm{lcm}(p^n - 1, q^n - 1)$.

(1) If $v_2(p^n - 1) = v_2(q^n - 1)$, then

$$\frac{T}{2} \equiv \frac{p^n - 1}{2} \,(\mathrm{mod}\, p^n - 1) \quad \text{and} \quad \frac{T}{2} \equiv \frac{q^n - 1}{2} \,(\mathrm{mod}\, q^n - 1),$$

and so we have

$$x^{\frac{T}{2}} \equiv -1 \bmod (f(x), p) \text{ and } x^{\frac{T}{2}} \equiv -1 \bmod (f(x), q).$$

By the Chinese Remainder Theorem, we get

$$x^{\frac{T}{2}} \equiv pq - 1 \bmod (f(x), pq).$$

Thus $S = T/2$ and $C = pq - 1$ are desirable integers.

(2) If $v_2(p^n - 1) > v_2(q^n - 1)$, then we have

$$x^{\frac{T}{2}} \equiv -1 \bmod (f(x), p) \text{ and } x^{\frac{T}{2}} \equiv 1 \bmod (f(x), q).$$

By Lemma 15, we get

$$\begin{aligned} x^{\frac{T}{2}} &\equiv \left[(1-(p-1)) \cdot \left[p^{-1}\right]_{\bmod q}\right]_{\bmod q} \cdot p + (p-1) \\ &\equiv \left[2 \cdot \left[p^{-1}\right]_{\bmod q} - 1\right]_{\bmod q} \cdot p + (p-1) \bmod (f(x), pq). \end{aligned}$$

Since $\left[p^{-1}\right]_{\bmod q} > \frac{q}{2}$, it follows that

$$\left[2 \cdot \left[p^{-1}\right]_{\bmod q} - 1\right]_{\bmod q} = 2 \cdot \left[p^{-1}\right]_{\bmod q} - q - 1$$

is an even number, and so $S = T/2$ and $C = \left[2 \cdot \left[p^{-1}\right]_{\bmod q} - 1\right]_{\bmod q} \cdot p + (p-1)$ are desirable integers.

(3) The proof is similar to (2). ■

The following corollary immediately follows from Theorem 3 and Lemma 16.

Corollary 17 *Let p and q be two odd prime numbers with $p < q$ and $f(x)$ be a primitive polynomial of degree $n \geq 2$ over $\mathbf{Z}/(pq)$. Set $T = \operatorname{lcm}(p^n - 1, q^n - 1)$,*

$$E_1 = \frac{(p-1) \cdot (q-1) \cdot (pq)^{\frac{n}{2}}}{1 - \frac{p-1}{p^n-1} - \frac{q-1}{q^n-1}}, \quad \text{and } E_2 = \left\lfloor \frac{q}{p} \right\rfloor \cdot \operatorname{lcm}\left(p^n - 1, \frac{q^n-1}{q-1}\right).$$

If one of the following three conditions is satisfied:

(1) $v_2(p^n-1) = v_2(q^n-1)$ *and* $T > \max\{E_1, E_2\}$;

(2) $v_2(p^n-1) > v_2(q^n-1)$, $[p^{-1}]_{\bmod q} > \frac{q}{2}$ *and* $T > E_1$;

(3) $v_2(p^n-1) < v_2(q^n-1)$, $[q^{-1}]_{\bmod p} > \frac{p}{2}$ *and* $T > E_1$,

then for $\underline{a}, \underline{b} \in G'(f(x), pq)$, $\underline{a} = \underline{b}$ *if and only if* $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$.

We compared the proportion of (n, p, q) satisfying the conditions of Corollary 17 and the proportion of (n, p, q) satisfying the conditions of Theorem 1 in [18], and results are listed in Table 3. Though the conditions of Corollary 17 is stronger than the conditions of Theorem 3, it can be seen that the proportion of (n, p, q) satisfying the conditions of Corollary 17 is still higher than that of Theorem 1 in [18]. This again confirms that the main result of this paper, i.e., Theorem 3, is really an improvement of Theorem 1 in [18].

Table 3 Comparison between the proportion of (n, p, q) satisfying the conditions of Corollary 17 and those of Theorem 1 in [18]

n	Corollary 17			Theorem 1 in [18]		
	$3 \le p < q \le prime(k)$			$3 \le p < q \le prime(k)$		
	$k = 1000$	$k = 3000$	$k = 5000$	$k = 1000$	$k = 3000$	$k = 5000$
$2 \le n \le 31$	63.847%	64.106%	64.284%	49.538%	49.730%	49.756%
$3 \le n \le 31$	66.049%	66.316%	66.501%	50.811%	51.003%	51.031%
$4 \le n \le 31$	66.054%	66.319%	66.501%	49.633%	49.826%	49.860%
$5 \le n \le 31$	66.067%	66.322%	66.503%	51.158%	51.355%	51.388%
$6 \le n \le 31$	66.039%	66.309%	66.494%	49.679%	49.867%	49.897%
$7 \le n \le 31$	66.058%	66.317%	66.500%	51.325%	51.514%	51.545%

References

[1] M. Ward, The arithmetical theory of linear recurring series, Trans. Amer. Math. Soc. 35 (1933) 600-628.

[2] M.Q. Huang, Analysis and cryptologic evaluation of primitive sequences over an integer residue ring, PhD dissertation, Graduate School of USTC, Academia Sinica, Beijing, China, 1988.

[3] M.Q. Huang and Z.D. Dai, Projective maps of linear recurring sequences with maximal p-adic periods, Fibonacci Quart. 30 (1992) 139-143.

[4] Z.D. Dai, T. Beth and D. Gollman, Lower bounds for the linear complexity of sequences over residue ring, in: Advances in Cryptology EUROCRYPT'90, in: Lecture Notes in Comput. Sci., vol. 473, Springer-Verlag, Berlin, 1991, pp. 189-195.

[5] Z.D. Dai, Binary sequences derived from ML-sequences over rings I: periods and minimal polynomials, J. Crypt. 5 (1992) 193-207.

[6] A.S. Kuzmin and A.A. Nechaev, Linear recurring sequences over Galois ring, Russian Math. Surveys 48 (1993) 171–172.

[7] A.S. Kuzmin, Lower estimates for the ranks of coordinate sequences of linear recurrent sequences over primary residue rings of integers, Russian Mathematical Surveys 48 (1993) 203-204.

[8] W.F. Qi, J.H. Yang and J.J. Zhou, ML-sequences over rings $\mathbf{Z}/(2^e)$, in: Advances in Cryptology ASIACRYPT'98, in: Lecture Notes in Comput. Sci., vol. 1514, Springer-Verlag, Berlin, 1998, pp. 315–325.

[9] W.F. Qi and X.Y. Zhu, Compressing mappings on primitive sequences over $\mathbf{Z}/(2^e)$ and its Galois extension, Finite Fields Appl. 8 (2002) 570-588.

[10] X.Y. Zhu and W.F. Qi, Comprssion mappings on primitive sequences over $\mathbf{Z}/(p^e)$, IEEE Trans. Inform. Theory 50 (2004) 2442-2448.

[11] X.Y. Zhu and W.F. Qi, Further result of compressing maps on primitive sequences modulo odd prime powers, IEEE Trans. Inform. Theory 53 (2007) 2985-2990.

[12] X.Y. Zhu and W.F. Qi, Uniqueness of the distribution of zeroes of primitive level sequences over $\mathbf{Z}/(p^e)$, Finite Fields Appl. 11 (2005) 30-44.

[13] X.Y. Zhu and W.F. Qi, Uniqueness of the distribution of zeroes of primitive level sequences over $\mathbf{Z}/(p^e)$ (II), Finite Fields Appl. 13 (2007) 230-248.

[14] T.Tian and W.F. Qi, Injectivity of compressing maps on primitive sequences over $\mathbf{Z}/(p^e)$, IEEE Trans. Inform. Theory 53 (2007) 2966-2970.

[15] Q.X. Zheng and W.F. Qi, Distribution properties of compressing sequences derived from primitive sequences over $\mathbf{Z}/(p^e)$, IEEE Trans. Inform. Theory 56 (2010) 555-563.

[16] X.Y. Zhu and W.F. Qi, On the distinctness of modular reductions of maximal length sequences modulo odd prime powers, Math. Comp. 77 (2008) 1623–1637.

[17] A. Klapper and M. Goresky, 2-Adic shift registers, in: Proc. of 1993 Cambridge Security Workshop, Fast Software Encryption, in: Lecture Notes in Comput. Sci., vol. 809, Springer-Verlag, New York, 1993, pp. 174–178.

[18] H.J. Chen and W.F. Qi, On the distinctness of maximal length sequences over $\mathbf{Z}/(pq)$ modulo 2, Finite Fields Appl. 15 (2009) 23-39.

[19] H.L. Garner, The residue number system, IRE. Trans. Elec. Comput. 8 (1959) 140-147.