Cryptogr. Commun. (2016) 8:371–381
DOI 10.1007/s12095-015-0151-8

On the distinctness of primitive sequences over $\mathbf{Z}/(p^e q)$ modulo 2

Yuan Cheng[1] · Wen-Feng Qi[1] · Qun-Xiong Zheng[1] · Dong Yang[1]

Received: 12 July 2014 / Accepted: 13 July 2015 / Published online: 7 August 2015

Abstract Let N be an integer greater than 1 and $\mathbf{Z}/(N)$ the integer residue ring modulo N. Extensive experiments seem to imply that primitive sequences of order $n \geq 2$ over $\mathbf{Z}/(N)$ are pairwise distinct modulo 2. However, efforts to obtain a formal proof have not been successful except for the case when N is an odd prime power integer. Recent research has mainly focussed on the case of square-free odd integers with several special conditions. In this paper we study the problem over $\mathbf{Z}/(p^e q)$, where p and q are two distinct odd primes, e is an integer greater than 1. We provide a sufficient condition to ensure that primitive sequences generated by a primitive polynomial over $\mathbf{Z}/(p^e q)$ are pairwise distinct modulo 2.

Keywords Linear recurring sequences · Modular reductions · Integer residue rings · Primitive polynomials · Primitive sequences

Mathematics Subject Classification (2010) 11B50 · 94A55 · 94A60

✉ Wen-Feng Qi
wenfeng.qi@263.net

Yuan Cheng
yuancheng61@163.com

Qun-Xiong Zheng
qunxiong_zheng@163.com

Dong Yang
yangdongsky@126.com

[1] State Key Laboratory of Mathematical Engineering and Advanced Computing, Zhengzhou Information Science and Technology Institute, Zhengzhou, People's Republic of China

1 Introduction

Throughout the paper, for any integer $N \geq 2$, let $\mathbf{Z}/(N)$ be the integer residue ring modulo N. We always choose $\{0, 1, ..., N-1\}$ as the representatives of the ring $\mathbf{Z}/(N)$. Thus a sequence $\underline{a}$ over $\mathbf{Z}/(N)$ is usually viewed as an integer sequence over $\{0, 1, ..., N-1\}$. Moreover, for an integer a and a positive integer $b \geq 2$, we denote the least nonnegative residue of a modulo b by $[a]_{\bmod b}$. Similarly, for an integer sequence $\underline{a} = (a(t))_{t\geq 0}$, we denote $[\underline{a}]_{\bmod b} = ([a(t)]_{\bmod b})_{t\geq 0}$.

In September 2011, a set of two cryptographic algorithms was accepted by 3GPP SA3 as a new inclusion in the LTE standards. It consists of a confidentiality algorithm named 128-EEA3 and an integrity algorithm named 128-EIA3, both of which are based on a core stream cipher algorithm named ZUC [1]. ZUC algorithm adopts primitive sequences over the prime field $\mathbf{Z}/(2^{31}-1)$ as driving sequences. Cryptographic analyses [1, Section 12] show that those driving sequences have a significant contribution to algorithm's resistance against bit-oriented cryptographic attacks, including fast correlation attacks, linear distinguishing attacks and algebraic attacks. Note that we can derive 31 sequences totally from the 2-adic expansion of $\underline{a} = \underline{a}_0 + \underline{a}_1 \cdot 2 + \cdots + \underline{a}_{30} \cdot 2^{30}$, called the 2-adic coordinate sequences of $\underline{a}$. The essential rationality for the application of primitive sequences over $\mathbf{Z}/(2^{31}-1)$ is that they are pairwise distinct modulo 2 [3, Theorem 4.2] i.e. $\underline{a} = \underline{b}$ iff $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$, where $\underline{a}$ and $\underline{b}$ are two primitive sequences over $\mathbf{Z}/(2^{31}-1)$ generated by a primitive polynomial. Such "distinctness property" guarantees that the 31 binary sequences $\underline{a}_0, \ldots, \underline{a}_{30}$ have the following two important properties: (1) all of their periods are equal to the period of $\underline{a}$; (2) each $\underline{a}_k$ uniquely determine the original primitive sequence $\underline{a}$, see [1 Page18] and [2, Corollary 1, Remark 1] for more details.

Generally, for an integer $e \geq 2$, if primitive sequences (its definition is given in Subsection 2.1) over $\mathbf{Z}/(2^e-1)$ are pairwise distinct modulo 2, then their 2-adic coordinate sequences also enjoy the two properties as mentioned above. We note that, however, primitive sequences over $\mathbf{Z}/(2^e-1)$ are not always pairwise distinct modulo 2. For example, $\underline{a} = (1, 5, 4, 20, 16, 17, \ldots)$ and $\underline{b} = (11, 13, 2, 10, 8, 19, \ldots)$ are two distinct primitive sequences of order 1 generated by $x-5$ over $\mathbf{Z}/(2^6-1)$, it is easy to verify that $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$. On the other hand, to the best of our knowledge, no counterexample has been found until now if the order of primitive sequences is greater than 1. It seems to imply that primitive sequences of order $n \geq 2$ over $\mathbf{Z}/(2^e-1)$ are pairwise distinct modulo 2. Unfortunately, efforts to obtain a formal proof have not been successful.

Recent study indicates that the problem of modulo-2 distinctness over $\mathbf{Z}/(2^e-1)$ seems not easier than over $\mathbf{Z}/(N)$ except for some special e (see, for example, [2]), where N is an odd integer. Additionally, since whether the property of modulo-2 distinctness holds for $\mathbf{Z}/(N)$ is also of interest in mathematics, the study of modulo-2 distinctness over $\mathbf{Z}/(2^e-1)$ is generally turned to the case of $\mathbf{Z}/(N)$.

The known results for the problem over $\mathbf{Z}/(N)$ mainly rely on the factorization of N. The case that N is an odd prime power integer has been completely solved in [3].

Theorem 1 *([3, Theorem 4.2]) Let p^e be an odd prime power and $f(x)$ a primitive polynomial of degree n over $\mathbf{Z}/(p^e)$. Then $\underline{a} = \underline{b}$ iff $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$, where $\underline{a}$ and $\underline{b}$ are two primitive sequences generated by $f(x)$ over $\mathbf{Z}/(p^e)$.*

Besides, several results for square-free N can be found in [4–8]. But there is no known result in the case when N is neither square-free nor prime power.

This paper studies the problem over $\mathbf{Z}/(p^e q)$, where p and q are two distinct odd primes, e is an integer greater than 1. Utilizing the same technology of decimation proposed in our previous work [9] and the Chinese Remainder Theorem, we provide a sufficient condition to ensure that primitive sequences generated by a primitive polynomial $f(x)$ over $\mathbf{Z}/(p^e q)$ are pairwise distinct modulo 2, see Theorem 2 for details.

The rest of the paper is organized as follows. In Section 2 we present some necessary preliminaries. In Section 3 we establish the main results of this paper.

2 Preliminaries

2.1 Primitive polynomials and primitive sequences

Let N be an integer greater than 1. If a sequence $\underline{a}$ over $\mathbf{Z}/(N)$ satisfies

$$a(i+n) = [c_{n-1}a(i+n-1) + \ldots + c_1 a(i+1) + c_0 a(i)] \bmod N$$

for any integer $i \geq 0$, where n is a positive integer and $c_0, c_1, \ldots, c_{n-1} \in \mathbf{Z}/(N)$ are constant coefficients, then $\underline{a}$ is called a *linear recurring sequence* of order n over $\mathbf{Z}/(N)$ generated by $f(x) = x^n - c_{n-1}x^{n-1} - \ldots - c_0$ (or $\underline{a}$ is a sequence of order n over $\mathbf{Z}/(N)$ for simplicity), and $f(x)$ is called a characteristic polynomial of $\underline{a}$. A characteristic polynomial of $\underline{a}$ with the least degree is called a minimal polynomial. Note that, generally speaking, a minimal polynomial of a sequence over $\mathbf{Z}/(N)$ is not necessarily unique. For example, both $x^2 - x - 1$ and $x^2 - 4x - 1$ are the minimal polynomials of the sequence $(0, 3, 3, 6, 0, 6, 6, 3, ...)$ over $\mathbf{Z}/(9)$ whose period is equal to 8. For convenience, the set of sequences generated by $f(x)$ over $\mathbf{Z}/(N)$ is generally denoted by $G(f(x), N)$.

Let $f(x)$ be a monic polynomial of degree n over $\mathbf{Z}/(N)$. If $f(0)$ is an invertible element in $\mathbf{Z}/(N)$, that is $\gcd(f(0), N) = 1$, then there exists a positive integer T such that $x^T - 1$ is divisible by $f(x)$ in $\mathbf{Z}/(N)[x]$. The minimum of such T is called the period of $f(x)$ over $\mathbf{Z}/(N)$ and denoted by $per(f(x), N)$. In the case when N is a prime power integer, say $N = p^e$, it is known that $per(f(x), p^e) \leq p^{e-1}(p^n - 1)$, see [10]. If $per(f(x), p^e) = p^{e-1}(p^n - 1)$, then $f(x)$ is called a *primitive polynomial* of order n over $\mathbf{Z}/(p^e)$. A sequence $\underline{a}$ over $\mathbf{Z}/(p^e)$ is called a *primitive sequence* of order n if $\underline{a}$ is generated by a primitive polynomial of degree n over $\mathbf{Z}/(p^e)$ and $[\underline{a}] \bmod p$ is not an all-zero sequence. In the case when N is an arbitrary integer, assume $N = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ is the canonical factorization of N. A monic polynomial $f(x)$ of degree n over $\mathbf{Z}/(N)$ is called a *primitive polynomial* if for every $i \in \{1, 2, \ldots, r\}$, $f(x) (\mathrm{mod} p_i^{e_i})$ is a primitive polynomial of degree n over $\mathbf{Z}/(p_i^{e_i})$. A sequence $\underline{a}$ over $\mathbf{Z}/(N)$ is called a *primitive sequence* of order n if $\underline{a}$ is generated by a primitive polynomial of degree n over $\mathbf{Z}/(N)$ and $[\underline{a}] \bmod p_i$ is not an all-zero sequence for every $i \in \{1, 2, \ldots, r\}$, that is, $[\underline{a}] \bmod p_i^{e_i}$ is a primitive sequence of order n over $\mathbf{Z}/(p_i^{e_i})$. For convenience, the set of primitive sequences generated by a primitive polynomial $f(x)$ over $\mathbf{Z}/(N)$ is generally denoted by $G'(f(x), N)$.

2.2 Element distribution properties of sequences over $\mathbf{Z}/(p^e)$

Let p^e be a prime power integer. For a sequence $\underline{a} = (a(t))_{t \geq 0}$ over $\mathbf{Z}/(p^e)$, if we write each $a(t)$ in its unique p-adic expansion as $a(t) = a_0(t) + a_1(t) \cdot p + \ldots + a_{e-1}(t) \cdot p^{e-1}$, where

$a_i(t) \in \{0, 1, \ldots, p-1\}$ for $i \in \{0, 1, \ldots, e-1\}$, then the p-ary sequence $\underline{a}_i = (a_i(t))_{t\geq 0}$ is called the i-th coordinate sequence of $\underline{a}$.

It is clear that if $f(x)$ is a polynomial over $\mathbf{Z}/(p^e)$, then $f(x)$ is also a polynomial over $\mathbf{Z}/(p^i)$ with its coefficients modulo p^i for $1 \leq i \leq e-1$.

Definition 1 A monic polynomial $f(x)$ of degree n over $\mathbf{Z}/(p^e)$ is called a basic irreducible polynomial if $f(x)$ is an irreducible polynomial of degree n over $\mathbf{Z}/(p)$.

Remark 1 Basic irreducible polynomials are also called Galois polynomials, for example, see [12].

If $f(x)$ is a basic irreducible polynomial over $\mathbf{Z}/(p^e)$, then it is clear that $f(x)$ is also a basic irreducible polynomial over $\mathbf{Z}/(p^i)$ for $1 \leq i \leq e-1$. Moreover, any primitive polynomial over $\mathbf{Z}/(p^e)$ is a basic irreducible polynomial over $\mathbf{Z}/(p^e)$, but the converse is not true.

We first present an element distribution property for linear recurring sequences generated by basic irreducible polynomials over $\mathbf{Z}/(p^e)$.

Lemma 1 *([11, Proposition 1]) Let $f(x)$ be a basic irreducible polynomial of degree n over $\mathbf{Z}/(p^e)$ and $\underline{a} \in G(f(x), p^e)$ with $\underline{a}_0 \neq \underline{0}$, where $\underline{a}_0$ is the 0-th coordinate sequence of $\underline{a}$. If*

$$per\,(f(x), p) \geq \left(p^e - 1\right) p^{n/2+e-1},$$

then every element of $\mathbf{Z}/(p^e)$ appears at least once in $\underline{a}$.

For a sequence $\underline{a} = (a(t))_{t\geq 0}$ and a positive integer s, we denote by $\underline{a}^{(s)}$ the s-fold decimation of $\underline{a}$, i.e. $\underline{a}^{(s)} = (a(st))_{t\geq 0}$. Next we will show that if $\underline{a}$ is a primitive sequence of order n over $\mathbf{Z}/(p^e)$ and s is a positive integer satisfying $\frac{p^n-1}{\gcd(p^n-1,s)} > p^{n/2}$, then the minimal polynomial of $\underline{a}^{(s)}$ over $\mathbf{Z}/(p^e)$ is unique and is a basic irreducible polynomial of degree n.

Proposition 1 *Let p^e be a prime power and $f(x)$ a primitive polynomial of degree n over $\mathbf{Z}/(p^e)$. Let $\underline{a} \in G'(f(x), p^e)$ and s a positive integer. If*

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

then the minimal polynomial of $\underline{a}^{(s)}$ over $\mathbf{Z}/(p^e)$ is unique and is a basic irreducible polynomial of degree n only depending on $f(x)$. Moreover, let $g(x)$ be the minimal polynomial of $\underline{a}^{(s)}$ over $\mathbf{Z}/(p^e)$. Then

$$per\left(g(x), p^e\right) = \frac{p^{e-1}(p^n-1)}{\gcd\left(p^{e-1}(p^n-1), s\right)} \text{ and } per\,(g(x), p) = \frac{p^n - 1}{\gcd(p^n - 1, s)}.$$

Proof See Appendix A. □

Combining Lemma 1 with Proposition 1, we can immediately obtain Lemma 2 as follows.

Lemma 2 *Let $f(x)$ be a primitive polynomial of degree $n \geq 2$ over $\mathbf{Z}/(p^e)$ and $\underline{a} \in G'(f(x), p^e)$. Let s be a positive integer. If*

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

then every element of $\mathbf{Z}/(p^e)$ appears at least once in $\underline{a}^{(s)}$.

Let $\underline{a} = (a(t))_{t\geq 0}$ and $\underline{b} = (b(t))_{t\geq 0}$ be two sequences over $\mathbf{Z}/(p^e)$. If there exists $u, v \in \mathbf{Z}/(p^e)$, not both equal to 0, such that $[u \cdot \underline{a} + v \cdot \underline{b}]_{\bmod p^e} = \underline{0}$, that is $[u \cdot a(t) + v \cdot b(t)]_{\bmod p^e} = 0$ for any integer $t \geq 0$, then we say that $\underline{a}$ and $\underline{b}$ are linearly dependent over $\mathbf{Z}/(p^e)$. Otherwise, we say that $\underline{a}$ and $\underline{b}$ are linearly independent over $\mathbf{Z}/(p^e)$. For the case when $e = 1$, if $\underline{a}$ and $\underline{b}$ are linearly dependent over $\mathbf{Z}/(p)$, and additionally $\underline{b} \neq \underline{0}$, then it follows that $\underline{a} = [\lambda \cdot \underline{b}]_{\bmod p}$ for some $\lambda \in \mathbf{Z}/(p)$. However, this is not true for the case when $e > 1$. For instance, let $\underline{a} = (0, 1, 2, 3, \ldots)$ and $\underline{b} = (3, 2, 1, 0, \ldots)$ be two sequences with period 4 over $\mathbf{Z}/(9)$, it is easy to verify that $\underline{a}$ and $\underline{b}$ are linearly dependent over $\mathbf{Z}/(9)$, but there does not exist $\lambda \in \mathbf{Z}/(9)$ such that $\underline{a} = [\lambda \cdot \underline{b}]_{\bmod 9}$.

We now present an element distribution property for two linearly independent sequences over $\mathbf{Z}/(p^e)$.

Lemma 3 *([12, Corollary 5]) Let $f(x)$ be a basic irreducible polynomial of degree n over $\mathbf{Z}/(p^e)$ and $\underline{a}, \underline{b} \in G(f(x), p^e)$. If $\underline{a}$ and $\underline{b}$ are linearly independent over $\mathbf{Z}/(p^e)$ and*

$$per\left(f(x), p\right) \geq \left(p^{2e} - 1\right) p^{n/2+e-1},$$

then for any $u, v \in \mathbf{Z}/(p^e)$, there exists an integer $t \geq 0$ such that $a(t) = u, b(t) = v$.

Combining Lemma 3 with Proposition 1, we can immediately obtain Lemma 4 as follows.

Lemma 4 *Let $f(x)$ be a primitive polynomial of degree n over $\mathbf{Z}/(p^e)$ and $\underline{a}, \underline{b} \in G'(f(x), p^e)$. Let s be a positive integer. If $\underline{a}^{(s)}$ and $\underline{b}^{(s)}$ are linearly independent over $\mathbf{Z}/(p^e)$ and*

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

then for any $u, v \in \mathbf{Z}/(p^e)$, there exists an integer $t \geq 0$ such that $a^{(s)}(t) = u, b^{(s)}(t) = v$.

3 Distinctness of primitive sequences over $\mathbf{Z}/(p^e q)$ modulo 2

Throughout this section, we always assume that p and q are two fixed distinct odd primes, e is an integer greater than 1.

We make our main result explicit in the following statement.

Theorem 2 *Let $f(x)$ be a primitive polynomial of degree $n \geq 2$ over $\mathbf{Z}/(p^e q)$. If both of the following two conditions hold:*
(i) $\frac{p^n-1}{\gcd(p^n-1, q^n-1)} \geq (p^e - 1) p^{(n/2+e-1)}$,
(ii) $\frac{q^n-1}{\gcd(q^n-1, p^{e-1}(p^n-1))} \geq \left(q^2 - 1\right) q^{n/2}$,
then for $\underline{a}, \underline{b} \in G'(f(x), p^e q)$, $\underline{a} = \underline{b}$ if and only if $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$.

Proof The necessary condition is trivial. It suffices to prove that, under the above two conditions, $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$ implies that $\underline{a} = \underline{b}$. □

Let $\underline{a}, \underline{b} \in G'(f(x), p^e q)$ be distinct primitive sequences with $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$. Then we will show a contradiction. Using the Chinese Remainder Theorem we have

$$\underline{a} = \left[q \cdot \underline{u}_a + p^e \cdot \underline{v}_a\right]_{\bmod p^e q}, \tag{1}$$

$$\underline{b} = \left[q \cdot \underline{u}_b + p^e \cdot \underline{v}_b\right]_{\bmod p^e q}, \tag{2}$$

where $\underline{u}_a, \underline{u}_b \in G'(f(x), p^e)$ and $\underline{v}_a, \underline{v}_b \in G'(f(x), q)$.

Case 1: $\underline{u}_a = \underline{u}_b$ and $\underline{v}_a \neq \underline{v}_b$

By Theorem 1, there exists an integer $t \geq 0$ such that

$$[v_a(t)]_{\bmod 2} \neq [v_b(t)]_{\bmod 2}. \tag{3}$$

Let $L^t \underline{u}_a = (u_a(t+s))_{s \geq 0}$ be the t-shift of $\underline{u}_a$. Then it is clear that $L^t \underline{u}_a \in G'(f(x), p^e)$. Let $\underline{c}$ be the $(q^n - 1)$-fold decimation of $L^t \underline{u}_a$, i.e.

$$\underline{c} = \left(u_a\left(t + k \cdot \left(q^n - 1\right)\right)\right)_{k \geq 0}.$$

Then by Condition (i) and Lemma 2, there exists an integer $k^* \geq 0$ such that $c(k^*) = 0$, which yields

$$u_a\left(t + k^* \cdot \left(q^n - 1\right)\right) = u_b\left(t + k^* \cdot \left(q^n - 1\right)\right) = 0.$$

Therefore, by (1) and (2) together with $per(\underline{v}_a) = per(\underline{v}_b) = q^n - 1$, we obtain that

$$\begin{aligned} a\left(t + k^* \cdot \left(q^n - 1\right)\right) &= p^e \cdot v_a\left(t + k^* \cdot \left(q^n - 1\right)\right) = p^e v_a(t), \\ b\left(t + k^* \cdot \left(q^n - 1\right)\right) &= p^e \cdot v_b(t + k^* \cdot \left(q^n - 1\right) = p^e v_b(t). \end{aligned}$$

Now (3) implies that

$$\left[a\left(t + k^* \cdot \left(q^n - 1\right)\right)\right]_{\bmod 2} \neq \left[b\left(t + k^* \cdot \left(q^n - 1\right)\right)\right]_{\bmod 2},$$

a contradiction.

Case 2: $\underline{u}_a \neq \underline{u}_b$ and $\underline{v}_a = \underline{v}_b$

By Theorem 1, there exists an integer $t \geq 0$ such that

$$[u_a(t)]_{\bmod 2} \neq [u_b(t)]_{\bmod 2}. \tag{4}$$

Set $\underline{c} = (v_a(t + k \cdot p^{e-1}(p^n - 1)))_{k \geq 0}$. Then it is clear that $\underline{c}$ is the $(p^{e-1}(p^n - 1))$-fold decimation of $L^t \underline{v}_a$. Employing Condition (i) and Lemma 2, we know that there exists an integer $k^* \geq 0$ such that $c(k^*) = 0$, which yields

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

Similar to Case 1, we can deduce that

$$\left[a(t + k^* \cdot p^{e-1}\left(p^n - 1\right)\right]_{\bmod 2} \neq \left[b(t + k^* \cdot p^{e-1}\left(p^n - 1\right)\right]_{\bmod 2},$$

which is a contradiction.

Case 3: $\underline{u}_a \neq \underline{u}_b$ and $\underline{v}_a \neq \underline{v}_b$

By Theorem 1, there exists an integer $t \geq 0$ such that

$$[u_a(t)]_{\bmod 2} \neq [u_b(t)]_{\bmod 2}. \tag{5}$$

Set

$$\underline{c} = \left(v_a\left(t + k \cdot \left(p^{e-1}\left(p^n - 1\right)\right)\right)\right)_{k\geq 0}$$

and

$$\underline{d} = \left(v_b\left(t + k \cdot \left(p^{e-1}\left(p^n - 1\right)\right)\right)\right)_{k\geq 0}.$$

Then $\underline{c}$ and $\underline{d}$ are the $\left(p^{e-1}\left(p^n - 1\right)\right)$-fold decimation of $L^t\underline{v}_a$ and $L^t\underline{v}_b$, respectively. According to the proof of Case 1, it suffices to prove that there exists an integer $k^* \geq 0$ such that $c(k^*) = d(k^*) = 0$. Consider the following two sub-cases.

(1) $\underline{c}$ and $\underline{d}$ are linearly independent over $\mathbf{Z}/(q)$.

By Condition (ii) and Lemma 4, there exists an integer $k^* \geq 0$ such that $c(k^*) = d(k^*) = 0$.

(2) $\underline{c}$ and $\underline{d}$ are linearly dependent over $\mathbf{Z}/(q)$.

Combining Condition (ii) and Proposition 1 we have $\underline{d} \neq \underline{0}$, and

$$\underline{c} = [\lambda \cdot \underline{d}]_{\bmod q}$$

for some $\lambda \in \mathbf{Z}/(q)$. Then by Condition (ii) and Lemma 2, there exists an integer $k^* \geq 0$ such that $d(k^*) = 0$, and hence $c(k^*) = 0$.

Combining all the cases, we finish our proof.

Remark 2 Under the same conditions of Theorem 2, for $\underline{a} \in G'(f(x), p^e q)$, we have

$$per([\underline{a}]_{\bmod 2}) = per(\underline{a}) = \mathrm{lcm}\left(p^{e-1} \cdot (p^n - 1), q^n - 1\right),$$

where $per(\underline{a})$ is the period of sequence $\underline{a}$. In fact, the last equality is obvious by the definition of primitive sequences. It suffices to show the first equality. Firstly, it is clear that $per([\underline{a}]_{\bmod 2}) \leq per(\underline{a})$. On the other hand, since $L^k\underline{a} \neq \underline{a}$ for $0 < k < per(\underline{a})$, where $L^k\underline{a} = (a(t + k))_{t\geq 0}$ is the k-shift of $\underline{a}$, it follows from Theorem 2 that $[L^k\underline{a}]_{\bmod 2} \neq [\underline{a}]_{\bmod 2}$ for $0 < k < per(\underline{a})$ which implies that $per([\underline{a}]_{\bmod 2}) \geq per(\underline{a})$.

Remark 3 When $n \leq 2(2e - 1)$, Condition (i) fails to hold. In fact, if $n \leq 2(2e - 1)$, we have (note that both p and q are odd)

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

Remark 4 The method above does not apply to the case of $\mathbf{Z}/(p^e q^r)$ if $r > 1$. The obstacle is that in the Case 3 of our proof, if $\underline{c}$ and $\underline{d}$ are linearly dependent over $\mathbf{Z}/(q^r)$ with $r > 1$, then it is not true that $\underline{c} = [\lambda \cdot \underline{d}]_{\bmod q^r}$ for some $\lambda \in \mathbf{Z}/(q^r)$.

The rest of this Section is devoted to the discussion of Conditions (i)-(ii) of Theorem 2.

When $e = 2$, the proportions of (p, q) satisfying Conditions (i) and (ii) of Theorem 2 among $3 \leq p \neq q \leq prime(5000)$ are tested under several ranges of n, where $prime(k)$ is the k-th prime number, see the results in Table 1.

Based on a result of Bugeaud, Corvaja and Zannier [13, Theorem 1], we will show that for given p, q, e, Conditions (i) and (ii) of Theorem 2 always hold for sufficiently large n.

Table 1 Proportions of (p, q) satisfying Conditions (i) and (ii) of Theorem 2 among $3 \leq p \neq q \leq prime(5000)$

n	$3 \leq p \neq q \leq prime(5000)$	n	$3 \leq p \neq q \leq prime(5000)$
7	91.130 %	19	99.999 %
8	69.485 %	20	99.958 %
9	99.493 %	21	99.999 %
10	99.015 %	22	99.992 %
11	99.987 %	23	100 %
12	99.044 %	24	99.969 %
13	99.999 %	25	99.999 %
14	99.978 %	26	100 %
15	99.991 %	27	99.999 %
16	99.914 %	28	99.998 %
17	99.999 %	29	99.999 %
18	99.914 %	30	99.975 %

Lemma 5 *(*[13, Theorem 1]*) If a and b are two multiplicatively independent integers greater than 1 (i.e. the only integer solution (x, y) of the equation $a^x b^y = 1$ is $(x, y) = (0, 0)$), then for any given real number $\varepsilon > 0$, there exists an integer N_ε such that*

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

for $n > N_\varepsilon$.

Theorem 3 *For given p, q, e, there exists an integer N such that Conditions (i) and (ii) of Theorem 2 always hold if $n > N$.*

Proof Since it is clear that p and q are multiplicatively independent, it follows from Lemma 5 that for a given real number $\varepsilon > 0$, there exists a positive number N_ε such that

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

for $n > N_\varepsilon$. Therefore, when $n > N_\varepsilon$, we have

$$\frac{p^n - 1}{\gcd(p^n - 1, q^n - 1)} > \frac{p^n - 1}{2^{\varepsilon \cdot n}}, \tag{6}$$

$$\frac{q^n - 1}{\gcd(q^n - 1,\, p^{e-1}(p^n - 1))} \geq \frac{q^n - 1}{p^{e-1}\gcd(p^n - 1, q^n - 1)} > \frac{q^n - 1}{p^{e-1}2^{\varepsilon \cdot n}}. \tag{7}$$

Choose $0 < \varepsilon < 1/2$, then it can be verified that

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

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

Therefore there exists an integer N' such that for $n > N'$,

$$\frac{p^n-1}{2^{\varepsilon\cdot n}} > \left(p^e-1\right)p^{(n/2+e-1)} \text{ and } \frac{q^n-1}{p^{e-1}2^{\varepsilon\cdot n}} > \left(q^2-1\right)q^{n/2}. \tag{8}$$

Set $N = \max\{N_\varepsilon, N'\}$. Then the result is obtained by combining (6), (7) and (8). □

Acknowledgments The authors would like to thank the anonymous referees for their helpful comments and suggestions. This work is supported by NSF of China (Grant Nos. 61272042 and 61402524) and by the Science and Technology on Information Assurance Laboratory (Grant No. KJ-13-006).

Appendix A: proof of Proposition 1

We first briefly introduce Galois rings. The notation and definitions we will use here are from [12].

A Galois ring is a finite commutative ring R with identity 1 in which the set of all zero divisors has the form pR for some prime p. Primary examples of Galois rings are integer residue rings $\mathbf{Z}/(p^e)$ and finite fields $GF(q)$ of q elements. A Galois ring R is uniquely determined up to isomorphism by its characteristic p^e and the number of elements q^e, where $q = p^r$. Therefore in what follows we denote such a ring by $GR(q^e, p^e)$. In particular, $GR(p^e, p^e) = \mathbf{Z}/(p^e)$. Let $R' = GR(q^{en}, p^e)$ be an extension of degree n of $R = GR(q^e, p^e)$. We denote by $\mathrm{Aut}\left(R'/R\right)$ the set of all automorphisms of the ring R' that fix each element of R. The group $\mathrm{Aut}\left(R'/R\right)$ is a cyclic group of order n generated by some automorphism σ:

$$\mathrm{Aut}\left(R'/R\right) =< \sigma >= \left\{1, \sigma, \ldots, \sigma^{n-1}\right\}.$$

Moreover, for $\alpha \in R'$, $\sigma(\alpha) = \alpha$ iff $\alpha \in R$, see [14, Theorem 14.30].

If $f(x)$ is a basic irreducible polynomial of degree n over $\mathbf{Z}/(p^e)$, then all the roots of $f(x)$ belong to $GR(p^{en}, p^e)$. Moreover if α is such a root in $GR(p^{en}, p^e)$, then $\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)$ are all the roots of $f(x)$ in $GR(p^{en}, p^e)$, where σ is the generator of the cyclic group $\mathrm{Aut}\left(GR(p^{en}, p^e)/GR(p^e, p^e)\right)$.

To prove Proposition 1, we need the following four lemmas.

Lemma 6 *([15, Theorem 2]) Let p^e be a prime power and $f(x)$ a monic polynomial of degree n over $\mathbf{Z}/(p^e)$ that has no multiple factors over $\mathbf{Z}/(p)$. Suppose $\alpha_0, \alpha_1, \ldots, \alpha_{n-1}$ are all roots of $f(x)$ in $GR(p^{em}, p^e)$ for some integer m. Then for any $\underline{a} = (a(t))_{t\geq 0} \in G(f(x), p^e)$, there uniquely exists $\beta_0, \beta_1, \ldots, \beta_{n-1} \in GR(p^{em}, p^e)$ such that*

$$a(t) = \beta_0\alpha_0^t + \beta_1\alpha_1^t + \ldots + \beta_{n-1}\alpha_{n-1}^t, t \geq 0. \tag{9}$$

Inversely, if a sequence $\underline{a} = (a(t))_{t\geq 0}$ over $\mathbf{Z}/(p^e)$ satisfies (9), then $\underline{a} \in G(f(x), p^e)$.

Lemma 7 *([16, Proposition 6.1]) Let p be a prime number and $f(x)$ a primitive polynomial of degree $n \geq 2$ over $\mathbf{Z}/(p)$. Let $\underline{a} \in G'(f(x), p)$ and s a positive integer. Then the minimal polynomial of $\underline{a}^{(s)}$ is irreducible over $\mathbf{Z}/(p)$ with degree dividing n and*

$$per\left(\underline{a}^{(s)}\right) = \frac{p^n-1}{\gcd(p^n-1, s)}.$$

Lemma 8 *([17, Theorem 2]) Let p^e be a prime power and $\underline{a} = (a(t))_{t\geq 0}$ a sequence over $\mathbf{Z}/(p^e)$. Then the minimal polynomial $g(x)$ of $\underline{a}$ over $\mathbf{Z}/(p^e)$ is unique iff $g(x)$ is a basic irreducible polynomial.*

Lemma 9 *([18, Theorem 11.1]) Let p^e be a prime power and $f(x)$ a basic irreducible polynomial of degree n over $\mathbf{Z}/(p^e)$. Suppose α is a root of $f(x)$ in $GR(p^{en}, p^e)$, then $per(f(x), p^e) = ord(\alpha)$, where $ord(\alpha)$ is the least positive integer s such that $\alpha^s = 1$.*

Now we start to prove Proposition 1.

Proof (Proof of Proposition 1) Let $g(x)$ be a minimal polynomial of $\underline{a}^{(s)}$ over $\mathbf{Z}/(p^e)$. Then it is clear that $g(x) \pmod p$ is a characteristic polynomial of $\left[\underline{a}^{(s)}\right]_{\bmod p}$ over $\mathbf{Z}/(p)$. By Lemma 8, it suffices to show that $g(x)$ is a basic irreducible polynomial polynomial of degree n over $\mathbf{Z}/(p^e)$ only depending on $f(x)$.

Let $h(x)$ be the minimal polynomial of $\left[\underline{a}^{(s)}\right]_{\bmod p}$ over $\mathbf{Z}/(p)$. Then it follows from Lemma 7 that $h(x)$ is irreducible over $\mathbf{Z}/(p)$ with degree dividing n and

$$per\left(\left[\underline{a}^{(s)}\right]_{\bmod\ p}\right) = \frac{p^n-1}{\gcd\left(p^n-1, s\right)}.$$

Since $\frac{p^n-1}{\gcd(p^n-1,s)} > p^{n/2}$ by assumption, it follows that $\deg h(x) = n$(for otherwise $\deg h(x) \le n/2$, which yields $per\left(\left[\underline{a}^{(s)}\right]_{\bmod p}\right) = per(h(x), p) \le p^{n/2}-1$, a contradiction). Since $g(x) \pmod p$ is a characteristic polynomial of $\left[\underline{a}^{(s)}\right]_{\bmod p}$ over $\mathbf{Z}/(p)$, we have

$$\deg g(x) = \deg\left(g(x) \pmod p\right) \ge \deg h(x) = n. \tag{10}$$

On the other hand, let $R' = GR\left(p^{en}, p^e\right)$, $R = \mathbf{Z}/(p^e)$, and $\mathrm{Aut}\left(R'/R\right) =< \sigma >$. Suppose α is a root of $f(x)$ in R', then $\alpha, \sigma(\alpha), \ldots, \sigma^{n-1}(\alpha)$ are all the roots of $f(x)$ in R'. By Lemma 6 there uniquely exist $\beta_0, \beta_1, \ldots, \beta_{n-1} \in R'$ such that

$$a(t) = \beta_0\alpha^t + \beta_1(\sigma(\alpha))^t + \ldots + \beta_{n-1}(\sigma^{n-1}(\alpha))^t \text{ for } t \ge 0,$$

and so

$$a^{(s)}(t) = a(st) = \beta_0(\alpha^s)^t + \beta_1(\sigma\left(\alpha^s\right))^t + \ldots + \beta_{n-1}(\sigma^{n-1}\left(\alpha^s\right))^t \text{ for } t \ge 0. \tag{11}$$

Let k be the least positive integer such that $\sigma^k(\alpha^s) = \alpha^s$. It is clear that $k \mid n$ and $\alpha^s, \sigma(\alpha^s), \ldots, \sigma^{k-1}(\alpha^s)$ are pairwise distinct. Then (11) can be rewritten as

$$a^{(s)}(t) = \beta'_0(\alpha^s)^t + \beta'_1(\sigma\left(\alpha^s\right))^t + \ldots + \beta'_{n-1}(\sigma^{k-1}\left(\alpha^s\right))^t \text{ for } t \ge 0,$$

where $\beta'_i = \sum_{j=0}^{(n/k)-1} \beta_{jk+i}$ for $0 \le i \le k-1$. Set

$$m(x) = \prod_{i=0}^{k-1}\left(x - \sigma^i\left(\alpha^s\right)\right).$$

Since $\sigma(m(x)) = m(x)$ and $m(x)$ is a monic polynomial over $\mathbf{Z}/(p^e)$, it follows from Lemma 6 that $m(x)$ is a characteristic polynomial of $\underline{a}^{(s)}$ over $\mathbf{Z}/(p^e)$, and so

$$\deg g(x) \le \deg m(x) = k \le n. \tag{12}$$

Combining (10) and (12) we obtain that $\deg g(x) = n$. Now we have

$$\deg\left(g(x) (\bmod\ p)\right) = \deg g(x) = n = \deg h(x),$$

it follows that both $g(x) \pmod p$ and $h(x)$ are the minimal polynomial of $\left[\underline{a}^{(s)}\right]_{\bmod p}$ over $\mathbf{Z}/(p)$, and so we get that $g(x) \pmod p = h(x)$ (since it is well-known that the minimal polynomial of a sequence over the finite field $\mathbf{Z}/(p)$ is unique). Thus we have showed that $g(x)$ is a basic irreducible polynomial of degree n over $\mathbf{Z}/(p^e)$, then by Lemma 8 the minimal polynomial of $\underline{a}^{(s)}$ over $\mathbf{Z}/(p^e)$ is unique. Moreover, it can be seen from the process of the proof above that $n = k$ and $g(x) = \prod_{i=0}^{n-1}\left(x - \sigma^i\left(\alpha^s\right)\right)$, and so $g(x)$ is obviously only depending on $f(x)$. Finally, by Lemma 9 we have

$$per(g(x), p^e) = ord(\alpha^s) = \frac{ord(\alpha)}{\gcd\left(ord(\alpha), s\right)} = \frac{per(f(x), p^e)}{\gcd\left(per(f(x), p^e), s\right)},$$

thus $per(g(x), p^e) = \frac{p^{e-1}(p^n-1)}{\gcd\left(p^{e-1}(p^n-1), s\right)}$. This completes the proof. □

References

1. ETSI/SAGE Specification: Specification of the 3GPP confidentiality and integrity algorithms 128-EEA3 & 128-EIA3. Document 4: Design and evaluation report; version: 2.0; Date: 9th Sep. 2011, Tech. rep., ETSI 2011. Available at: http://www.gsmworld.com/our-work/programmes-and-initiatives/fraud-and-security/gsm_security_algorithms.htm

2. Zheng, Q.X., Qi, W.F., Tian, T.: On the distinctness of modular reduction of primitive sequences over $\mathbf{Z}/(2^{32}-1)$. Des. Codes Crypt. **70**, 359–368 (2014)
3. Zhu, X.Y., Qi, W.F.: On the distinctness of modular reduction of maximal length modulo odd prime numbers. Math. Comput. **77**, 1623–1637 (2008)
4. Chen, H.J., Qi, W.F.: On the distinctness of maximal length sequences over $\mathbf{Z}/(pq)$ modulo 2. Finite Fields Appl **15**, 23–39 (2009)
5. Zheng, Q.X., Qi, W.F.: A new result on the distinctness of primitive sequences over $\mathbf{Z}/(pq)$ modulo 2. Finite Fields Appl **17**, 254–274 (2011)
6. Zheng, Q.X., Qi, W.F., Tian, T.: On the distinctness of binary sequences derived from primitive sequences modulo square-free odd integers. IEEE Trans. Inf. Theory **59**, 680–690 (2013)
7. Zheng, Q.X., Qi, W.F.: Further results on the distinctness of binary sequences derived from primitive sequences modulo square-free odd integers. IEEE Trans. Inf. Theory **59**, 4013–4019 (2013)
8. Hu, Z., Wang, L.: Injectivity of compressing maps on the set of primitive sequences modulo square-free odd integers. Cryptogr. Commun. (2015)
9. Yang, D., Qi, W.F., Zheng, Q.X.: Further results on the distinctness of modulo 2 reductions of primitive sequences over $\mathbf{Z}/(2^{32}-1)$. Des. Codes Crypt. **74**, 467–480 (2015)
10. Ward, M.: The arithmetical theory of linear recurring series. Trans. Am. Math. Soc. **35**, 600–628 (1933)
11. Bylkov, D.N., Kamlovskii, O.V.: Occurrence indices of elements in linear recurrence sequences over primary residue rings. Probl. Inf. Transm. **44**, 161–168 (2008)
12. Kamlovskii, O.V.: Frequency characteristics of linear recurrences over Galois rings. Matematicheskii Sbornik **200**, 31–52 (2009)
13. Bugeaud, Y., Corvaja, P., Zannier, U.: An upper bound for the G.C.D. of a^n-1 and b^n-1. Math. Z. **243**, 79–84 (2003)
14. Wan, Z.X.: Finite fields and Galois Rings. World Scientific Publisher, Singapore (2003)
15. Qi, W.F., Zhou, J.J.: Polynomial splitting ring and root representation of linear recurring sequences over $\mathbf{Z}/(p^e)$. Sci. China Ser **37**, 1047–1052 (1994)
16. Rueppel, R.A.: Analysis and Design of Stream Ciphers[M]. Springer Verlag, New York (1986)
17. Qi, W.F., Wang, J.L.: The Structure of Splitting Rings over $\mathbf{Z}/(p^e)$. Mathematica applicata **9**, 491–494 (1996)
18. Kurakin, V.L., Kuzmin, A.S., Mikhalev, A.V., Nechaev, A.A.: Linear recurring sequences over rings and modules. J. Math. Sci. **76**, 2793–2915 (1995)