Des. Codes Cryptogr. (2014) 70:359–368
DOI 10.1007/s10623-012-9698-y

On the distinctness of modular reductions of primitive sequences over $\mathbf{Z}/(2^{32}-1)$

Qun-Xiong Zheng · Wen-Feng Qi · Tian Tian

Received: 18 January 2012 / Revised: 2 May 2012 / Accepted: 11 May 2012 /
Published online: 30 May 2012

Abstract This paper studies the distinctness of modular reductions of primitive sequences over $\mathbf{Z}/(2^{32}-1)$. Let $f(x)$ be a primitive polynomial of degree n over $\mathbf{Z}/(2^{32}-1)$ and H a positive integer with a prime factor coprime with $2^{32}-1$. Under the assumption that every element in $\mathbf{Z}/(2^{32}-1)$ occurs in a primitive sequence of order n over $\mathbf{Z}/(2^{32}-1)$, it is proved that for two primitive sequences $\underline{a}=(a(t))_{t\geq 0}$ and $\underline{b}=(b(t))_{t\geq 0}$ generated by $f(x)$ over $\mathbf{Z}/(2^{32}-1)$, $\underline{a}=\underline{b}$ if and only if $a(t)\equiv b(t) \bmod H$ for all $t\geq 0$. Furthermore, the assumption is known to be valid for n between 7 and 100,000, the range of which is sufficient for practical applications.

Keywords Stream ciphers · Integer residue rings · Linear recurring sequences · Primitive sequences · Modular reductions

Mathematics Subject Classification 11B50 · 94A55 · 94A60

1 Introduction

The study of linear recurring sequences over integer residue rings started as early as 1920s. At first mathematicians were interested in their pure arithmetic properties [19–21]. Later on as the rise of cryptography, linear recurring sequences over $\mathbf{Z}/(p^e)$ were thought to be

Communicated by D. Panario.

Q.-X. Zheng · W.-F. Qi (✉) · T. Tian
Department of Applied Mathematics, Zhengzhou Information Science and Technology Institute, Zhengzhou, People's Republic of China
e-mail: wenfeng.qi@263.net

Q.-X. Zheng
e-mail: qunxiong_zheng@163.com

T. Tian
e-mail: tiantian_d@126.com

suitable for the design of stream ciphers, where p^e is a prime power. Then an enormous amount of effort has been directed toward the study of finding useful mappings to derive good pseudorandom sequences from linear recurring sequences over $\mathbf{Z}/(p^e)$, which are called compression mappings in literature, and proving that they are injective. Generally there are two kinds of compression mappings: one is based on e-variable functions over $\mathbf{Z}/(p)$ [2,9,12,14,15,17,25,26]; the other is based on mod H operation [27] , where H is an integer with a prime factor coprime with p. Besides, the pseudorandom properties of these compression sequences were also extensively studied, such as periodicity [5], linear complexity [4,11,13], and distribution properties [7,8,16,22].

Recently research interests on linear recurring sequences over $\mathbf{Z}/(p^e)$ are further extended to linear recurring sequences over $\mathbf{Z}/(M)$ [3,23,24], where M is a square-free odd integer. One of important reasons for this is that the period of a linear recurring sequence $\underline{a}$ of order n over $\mathbf{Z}/(p^e)$ is undesirable if $e \geq 2$. Recall that the period $per(\underline{a})$ is upbounded by $p^{e-1} \cdot (p^n - 1) \approx p^{e+n-1}$ [21]. It can be seen that for fixed p^e with $e \geq 2$, the period $per(\underline{a})$ increases slowly and far less than $p^{e \cdot n}$ as n increases. Therefore, to meet the requirement of long period in practical applications (such as $\geq 2^{64}$), n should be chosen large enough, which will be high resource consumption in hardware and software implementation. For example, to generate a sequence with period not less than 2^{64} over $\mathbf{Z}/(2^8)$, $\mathbf{Z}/(2^{16})$ and $\mathbf{Z}/(2^{32})$, the number of bit-registers required must be larger than 456, 784 and 1056, respectively. However for many square-free odd integers M, especially prime numbers M, linear recurring sequences over $\mathbf{Z}/(M)$ have no such periodic weakness. For cryptographic applications, the moduli of the form $2^e - 1$ have attracted much attention since the operation "mod $2^e - 1$" can be efficiently implemented both in hardware and software, and this offers new possibilities for advancement in the solution of applying linear recurring sequences over integer residue rings.

In Sep. 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 [6]. The ZUC algorithm adopts primitive sequences over the prime field $\mathbf{Z}/(2^{31}-1)$ as driving sequences. Cryptographic analyses [6, Section 12] have shown that those driving sequences have a significant contribution to the ZUC algorithm's resistance against bit-oriented cryptographic attacks, including fast correlation attacks, linear distinguishing attacks and algebraic attacks. In [27, Theorem 4.2] it was proved that if $\underline{a} = (a(t))_{t \geq 0}$ and $\underline{b} = (b(t))_{t \geq 0}$ are two primitive sequences over $\mathbf{Z}/(2^{31} - 1)$ generated by a primitive polynomial, then $\underline{a} = \underline{b}$ if and only if $a(t) \equiv b(t) \bmod 2$ for all $t \geq 0$, and we say that the modulo 2 reductions of primitive sequences over $\mathbf{Z}/(2^{31} - 1)$ are distinct. This is an important property for their cryptographic applications (see Remark 1).

Considering the operations over $\mathbf{Z}/(2^{32}-1)$ are more suitable to be implemented in 32-bit platforms than those over $\mathbf{Z}/(2^{31} - 1)$, we think that primitive sequences over $\mathbf{Z}/(2^{32} - 1)$ may substitute primitive sequences over $\mathbf{Z}/(2^{31} - 1)$ as a building block of stream ciphers if the distinctness of modulo 2 reductions also holds for primitive sequences over $\mathbf{Z}/(2^{32} - 1)$. In [24], this problem was partially answered by applying Theorem 20 to $M = 2^{32} - 1$. Through more careful study on the properties of primitive sequences over $\mathbf{Z}/(2^{32} - 1)$, in this paper the set of primitive sequences over $\mathbf{Z}/(2^{32} - 1)$ that can be proved to be distinct modulo 2 is greatly enlarged and almost includes all primitive sequences over $\mathbf{Z}/(2^{32} - 1)$. Moreover, such distinctness for "modulo 2" is further extended to "modulo H", where H is a positive integer with a prime factor coprime with $2^{32} - 1$. We remark that by the same method, similar results can be obtained for primitive sequences over $\mathbf{Z}/(2^4 - 1)$, $\mathbf{Z}/(2^8 - 1)$ and $\mathbf{Z}/(2^{16} - 1)$.

Throughout the paper we use the following notations. For any integer $N > 1$, let $\mathbf{Z}/(N)$ denote the integer residue ring modulo N. We always choose $\{0, 1, \ldots, N-1\}$ as the complete set of representatives for the elements of the ring $\mathbf{Z}/(N)$. Thus a sequence over $\mathbf{Z}/(N)$ is also seen as an integer sequence over $\{0, 1, \ldots, N-1\}$. For two integer sequences $\underline{a} = (a(t))_{t\geq 0}, \underline{b} = (b(t))_{t\geq 0}$ and a positive integer c, the congruence "$\underline{a} \equiv \underline{b} \bmod c$" means $a(t) \equiv b(t) \bmod c$ for all $t \geq 0$. Moreover, for any integer a and c, we denote the least nonnegative residue of a modulo c by $[a]_{\bmod c}$, and similarly, for an integer sequence $\underline{a}$, denote $\left[\underline{a}\right]_{\bmod c} = ([a(t)]_{\bmod c})_{t\geq 0}$.

2 Preliminaries

Let N be a positive integer greater than 1. If a sequence $\underline{a} = (a(t))_{t\geq 0}$ over $\mathbf{Z}/(N)$ satisfies the linear recurrence relation

$$a(t+n) \equiv c_{n-1} \cdot a(t+n-1) + \cdots + c_1 \cdot a(t+1) + c_0 \cdot a(t) \bmod N$$

for all $t \geq 0$, where n is a positive integer and $c_0, c_1, \ldots, c_{n-1} \in \mathbf{Z}/(N)$, then $\underline{a}$ is called a linear recurring sequence of order n over $\mathbf{Z}/(N)$ generated by $f(x) = x^n - c_{n-1}x^{n-1} - \cdots - c_0$. For convenience, the set of all linear recurring sequences generated by $f(x)$ over $\mathbf{Z}/(N)$ is denoted by $G(f(x), N)$. Particular interests for cryptography are the maximal period linear recurring sequences also called primitive sequences over $\mathbf{Z}/(N)$, which are generated by primitive polynomials over $\mathbf{Z}/(N)$. Next we introduce the definitions of primitive polynomials and primitive sequences over $\mathbf{Z}/(N)$.

First, assume N is a prime power, say $N = p^e$. Then a monic polynomial $f(x)$ of degree n over $\mathbf{Z}/(p^e)$ is called a primitive polynomial of degree n if the period of $f(x)$ over $\mathbf{Z}/(p^e)$ is equal to $p^{e-1}(p^n - 1)$, that is $p^{e-1}(p^n - 1)$ is the least positive integer P such that $x^P - 1$ is divisible by $f(x)$ in $\mathbf{Z}/(p^e)[x]$. 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 $\left[\underline{a}\right]_{\bmod p}$ is not an all-zero sequence. A primitive sequence $\underline{a}$ of order n over $\mathbf{Z}/(p^e)$ is (strictly) periodic and the period $per(\underline{a})$ is equal to $p^{e-1}(p^n - 1)$, see [21]. Second, assume $N = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ is the canonical factorization of N. Then a monic polynomial $f(x)$ of degree n over $\mathbf{Z}/(N)$ is called a primitive polynomial if for every $i \in \{1, 2, \ldots, r\}$, $f(x)$ 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 $\left[\underline{a}\right]_{\bmod p_i}$ is not an all-zero sequence for every $i \in \{1, 2, \ldots, r\}$, that is, $\left[\underline{a}\right]_{\bmod p_i^{e_i}}$ is a primitive sequence of order n over $\mathbf{Z}/(p_i^{e_i})$. It can be seen that the period of a primitive polynomial of degree n over $\mathbf{Z}/(N)$ and that of a primitive sequence of order n over $\mathbf{Z}/(N)$ are both equal to

$$\operatorname{lcm}\left(p_1^{e_1-1}\left(p_1^n - 1\right), p_2^{e_2-1}\left(p_2^n - 1\right), \ldots, p_r^{e_r-1}\left(p_r^n - 1\right)\right).$$

For convenience, the set of primitive sequences generated by a primitive polynomial $f(x)$ over $\mathbf{Z}/(N)$ is generally denoted by $G'(f(x), N)$. It is easy to see that for a primitive sequence $\underline{a} \in G'(f(x), N)$ and an integer c coprime with N, the sequence

$$\left[c \cdot \underline{a}\right]_{\bmod N} = \left([c \cdot a(t)]_{\bmod N}\right)_{t\geq 0}$$

is also a primitive sequence over $\mathbf{Z}/(N)$, i.e. $\left[c \cdot \underline{a}\right]_{\bmod N} \in G'(f(x), N)$.

Next we consider sequences over $\mathbf{Z}/(2^e - 1)$ and introduce their 2-adic coordinate sequences. For a sequence $\underline{a} = (a(t))_{t\geq 0}$ over $\mathbf{Z}/(2^e - 1)$, if we write every element $a(t)$ of $\underline{a}$ in its 2-adic expansion as

$$a(t) = a_0(t) + a_1(t) \cdot 2 + \cdots + a_{e-1}(t) \cdot 2^{e-1}, \quad t \geq 0,$$

then the binary sequence $\underline{a}_k = (a_k(t))_{t \geq 0}$ is called the kth 2-adic coordinate sequence of $\underline{a}$ for $0 \leq k \leq e-1$, and

$$\underline{a} = \underline{a}_0 + \underline{a}_1 \cdot 2 + \cdots + \underline{a}_{e-1} \cdot 2^{e-1}$$

is called the 2-adic expansion of $\underline{a}$. It is clear that $\underline{a}_0$ is in fact the modulo 2 reduction of $\underline{a}$, i.e., $\underline{a}_0 = \left[\underline{a}\right]_{\bmod 2}$. Moreover, if $\underline{b} = [2^i \cdot \underline{a}]_{\bmod 2^e-1}$ for some integer $1 \leq i \leq e-1$, then

$$\underline{b} = \underline{a}_{e-i} + \underline{a}_{e-i+1} \cdot 2 + \cdots + \underline{a}_{e-1} \cdot 2^{i-1} + \underline{a}_0 \cdot 2^i + \cdots + \underline{a}_{e-i-1} \cdot 2^{e-1}$$

is the 2-adic expansion of $\underline{b}$. It can be seen that the set of e 2-adic coordinate sequences of $\underline{b}$ is the same as the set of e 2-adic coordinate sequences of $\underline{a}$.

Finally, we discuss a simple property of primitive sequences over $\mathbf{Z}/(2^{32}-1)$. This is based on the following element distribution property of primitive sequences over a prime field of odd characteristic, whose proof follows from the same argument as used in [25, Lemma 4].

Lemma 1 *Let p be an odd prime number and $\underline{a}$ a primitive sequence over $\mathbf{Z}/(p)$ with period T. Then $a\,(t + T/2) \equiv -a\,(t) \bmod p$ for all $t \geq 0$.*

Let $p_1 = 3$, $p_2 = 5$, $p_3 = 17$, $p_4 = 257$ and $p_5 = 65537$. Then we have that $2^{32} - 1 = p_1 p_2 p_3 p_4 p_5$ which is the canonical factorization of $2^{32} - 1$. Note that $p_i = 2^{2^{i-1}} + 1$ for $1 \leq i \leq 5$, and so it follows from [18, Lemma 10] that for any positive integer n, we have that

$$v_2\left(p_i^n - 1\right) = \begin{cases} 2 + v_2\,(n)\,, & \text{if } i = 1 \text{ and } n \text{ is even,} \\ 2^{i-1} + v_2\,(n)\,, & \text{otherwise,} \end{cases} \tag{1}$$

where $v_2\,(k)$ denotes the greatest nonnegative integer m such that 2^m divides k. It can be seen that

$$v_2\left(p_i^n - 1\right) < v_2\left(p_5^n - 1\right) \quad \text{for} \quad 1 \leq i \leq 4. \tag{2}$$

Lemma 2 *Let $\underline{a}$ be a primitive sequence over $\mathbf{Z}/(2^{32}-1)$ with period T. Then we have that $a\,(t + T/2) \equiv 2^{16} \cdot a\,(t) \bmod 2^{32} - 1$ for all $t \geq 0$.*

Proof Note that $2^{16} \equiv 1 \bmod p_i$ for $1 \leq i \leq 4$ while $2^{16} \equiv -1 \bmod p_5$. It suffices to show that for all $t \geq 0$

$$a\,(t + T/2) \equiv a\,(t) \bmod p_i, 1 \leq i \leq 4 \tag{3}$$

and

$$a\,(t + T/2) \equiv -a\,(t) \bmod p_5. \tag{4}$$

Assume $\underline{a}$ is generated by a primitive polynomial of degree n over $\mathbf{Z}/(2^{32}-1)$. Then $T = \operatorname{lcm}\left(p_1^n - 1, p_2^n - 1, p_3^n - 1, p_4^n - 1, p_5^n - 1\right)$, and so it follows from (2) that

$$v_2\,(T) = v_2\left(p_5^n - 1\right) > v_2\left(p_i^n - 1\right) \quad \text{for} \quad 1 \leq i \leq 4,$$

which implies that

$$p_i^n - 1 \mid \frac{T}{2} \text{ for } 1 \leq i \leq 4, \tag{5}$$

while

$$\frac{T}{2} \equiv \frac{p_5^n - 1}{2} \bmod p_5^n - 1. \tag{6}$$

Note that $per([\underline{a}]_{\bmod p_i}) = p_i^n - 1$ for $1 \le i \le 5$. Hence (3) follows from (5), and (4) follows from (6) and Lemma 1. □

3 Main results

Given a positive integer n, the following assumption on primitive sequences of order n is important for our main result.

Assumption 1 (Element Distribution Assumption) If $\underline{a} = (a(t))_{t\ge 0}$ is a primitive sequence of order n over $\mathbf{Z}/(2^{32}-1)$ with period $per(\underline{a})$, then $a(t)$ runs through the set $\{0, 1, \ldots, 2^{32}-2\}$ as t runs from 0 to $per(\underline{a}) - 1$.

By applying [24, Theorem 11] to $M = 2^{32}-1$, we immediately get the following Theorem 1, which in fact gives a sufficient condition for n such that Assumption 1 is valid.

Theorem 1 [24, Theorem 11] *Let n be a positive integer and $2^{32} - 1 = p_1p_2p_3p_4p_5$ the canonical factorization of $2^{32} - 1$. Then Assumption 1 is valid for n if*

$$1 - \sum_{i=1}^{5} \frac{p_i - 1}{p_i^n - 1} > \sum_{k=2}^{5} \sum_{1\le i_1<\cdots<i_k\le 5} \frac{\prod_{j=1}^{k}(p_{i_j} - 1)p_{i_j}^{n/2}}{lcm\left(p_{i_1}^n - 1, p_{i_2}^n - 1, \ldots, p_{i_k}^n - 1\right)}. \tag{7}$$

Experimental data show that for $1 \le n \le 100000$, the inequality (7) always holds except $n = 1, 2, 3, 4$ and 6, which implies that Assumption 1 is valid if $7 \le n \le 100000$. This range of n is sufficient for practical applications. Furthermore, in theory it was proved that there exists an integer N (However, the value of N is not computable due to the ineffectivity of Diophantine Approximation, see [24, Proof of Theorem 13] and [1, Remarks (5)] for more details) such that Assumption 1 is valid for all $n > N$, see [24, Theorem 13].

Now we can make our main result explicit in the following statement.

Theorem 2 *Let $f(x)$ be a primitive polynomial of positive degree n over $\mathbf{Z}/(2^{32}-1)$, $\underline{a}, \underline{b} \in G'(f(x), 2^{32} - 1)$, and H a positive integer with a prime factor coprime with $2^{32} - 1$. If Assumption 1 is valid for n, then*

(i) $\underline{a} = \underline{b}$ *if and only if* $\underline{a} \equiv \underline{b} \bmod H$; *and*
(ii) $per\left([\underline{a}]_{\bmod H}\right) = per\left(\underline{a}\right)$.

With Theorem 2, it is easy to deduce some properties of 2-adic coordinate sequences of primitive sequences over $\mathbf{Z}/(2^{32} - 1)$.

Corollary 1 *Let $f(x)$ be a primitive polynomial of positive degree n over $\mathbf{Z}/(2^{32} - 1)$ and $\underline{a}, \underline{b} \in G'(f(x), 2^{32} - 1)$. If Assumption 1 is valid for n, then*

(i) for a given integer $k \in \{0, 1, \ldots, 31\}$, $\underline{a} = \underline{b}$ if and only if $\underline{a}_k = \underline{b}_k$; and
(ii) the period of every 2-adic coordinate sequence of $\underline{a}$ attains $per(\underline{a})$.

Proof

(i) Since the necessary condition is trivial, it suffices to show the sufficient condition. Let us denote

$$\underline{a}' = \left[2^{32-k} \cdot \underline{a}\right]_{\bmod 2^{32}-1} \text{ and } \underline{b}' = \left[2^{32-k} \cdot \underline{b}\right]_{\bmod 2^{32}-1}.$$

It is clear that $\underline{a}', \underline{b}' \in G'(f(x), 2^{32}-1)$. Since

$$\left[\underline{a}'\right]_{\bmod 2} = \underline{a}_k \text{ and } \left[\underline{b}'\right]_{\bmod 2} = \underline{b}_k,$$

it follows from Theorem 2 (i) that $\underline{a}' = \underline{b}'$, and so

$$\underline{a} = \left[r \cdot \underline{a}'\right]_{\bmod 2^{32}-1} = \left[r \cdot \underline{b}'\right]_{\bmod 2^{32}-1} = \underline{b},$$

where r is the multiplicative inverse of 2^{32-k} in $\mathbf{Z}/(2^{32}-1)$.

(ii) The result immediately follows from Theorem 2 (ii) and the fact that $\underline{a}_k$ is the modulo 2 reduction of the primitive sequence $[2^{32-k} \cdot \underline{a}]_{\bmod 2^{32}-1}$ for $0 \le k \le 31$.

□

Remark 1 If Assumption 1 is valid for n, then Corollary 1 implies that given a primitive polynomial $f(x)$ of degree n over $\mathbf{Z}/(2^{32}-1)$ and $\underline{a} \in G'(f(x), 2^{32}-1)$, theoretically there is an algorithm to recover $\underline{a}$ from any one of its 2-adic coordinate sequences. Thus it could be thought that every 2-adic coordinate sequence of $\underline{a}$ contains all the information of $\underline{a}$ and all 2-adic coordinate sequences of $\underline{a}$ are pairwise equivalent. Considering 2-adic coordinate sequences of sequences generated by a primitive polynomial or a T-function over $\mathbf{Z}/(2^{32})$, it is easily seen that such equivalence property does not hold, and so primitive sequences over $\mathbf{Z}/(2^{32}-1)$ exceeds them in this aspect and shall be interest for cryptographic applications. Please refer to [10] for sequences generated by T-functions.

Next we start to prove Theorem 2, we first give a necessary lemma.

Lemma 3 *Let $f(x)$ be a primitive polynomial of positive degree n over $\mathbf{Z}/(2^{32}-1)$, $\underline{a}, \underline{b} \in G'(f(x), 2^{32}-1)$, and h a prime number coprime with $2^{32}-1$. If Assumption 1 is valid for n and $\underline{a} \equiv \underline{b} \bmod h$, then there is a prime factor p of $2^{32}-1$ such that $\underline{a} \equiv \underline{b} \bmod p$.*

Proof Suppose $\underline{a} \not\equiv \underline{b} \bmod p$ for any prime factor p of $2^{32}-1$. It is clear that $\underline{c} = \left[\underline{a} - \underline{b}\right]_{\bmod 2^{32}-1}$ is a primitive sequence generated by $f(x)$ over $\mathbf{Z}/(2^{32}-1)$, i.e., $\underline{c} \in G'(f(x), 2^{32}-1)$. It follows from Assumption 1 that there is an integer $t^* \ge 0$ such that $c(t^*) = 1$, i.e., $a(t^*) - b(t^*) \equiv 1 \bmod 2^{32}-1$. Then either

$$a(t^*) = b(t^*) + 1 \text{ and } 0 \le b\left(t^*\right) < 2^{32} - 2 \tag{8}$$

or

$$a(t^*) = 0 \text{ and } b(t^*) = 2^{32} - 2. \tag{9}$$

Obviously, if $h \ge 3$, then both (8) and (9) imply that $a(t^*) \not\equiv b(t^*) \bmod h$, a contradiction to $\underline{a} \equiv \underline{b} \bmod h$. If $h = 2$, then $\underline{a} \equiv \underline{b} \bmod 2$ implies that only (9) holds. Denote by T the period of $f(x)$ over $\mathbf{Z}/(2^{32}-1)$. Then we have $per\left(\underline{a}\right) = per\left(\underline{b}\right) = T$. By applying Lemma 2 to (9) we get

$$a\left(t^* + T/2\right) = 0 \text{ and } b\left(t^* + T/2\right) = 2^{32} - 2^{16} - 1,$$

which yield

$$a\left(t^*+T/2\right)\equiv 0\not\equiv 1\equiv b\left(t^*+T/2\right) \bmod 2,$$

a contradiction to $\underline{a}\equiv\underline{b} \bmod 2$. Therefore, there at least exists a prime factor p of $2^{32}-1$ such that $\underline{a}\equiv\underline{b} \bmod p$. □

Proof (Proof of Theorem 2) (i) Since the necessary condition is trivial, in the following, we only prove the sufficient condition.

Suppose $\underline{a}\equiv\underline{b} \bmod H$ and h is a prime factor of H coprime with $2^{32}-1$. Then we also have $\underline{a}\equiv\underline{b} \bmod h$. If we denote by R the greatest factor of $2^{32}-1$ satisfying $\underline{a}\equiv\underline{b} \bmod R$, then by Lemma 3 we know $R>1$. In the following it suffices to show that $R=2^{32}-1$.

We continue the proof by contradiction. Suppose $R<2^{32}-1$.

First, let us denote $Q=\left(2^{32}-1\right)/R$. Then we have $Q>1$ and $\underline{a}\not\equiv\underline{b} \bmod q$ for any prime factor q of Q. Since $2^{32}-1$ is a square-free odd integer, it is clear that R and Q are also square-free odd integers and $\gcd(R,Q)=1$. By the Chinese Remainder Theorem, there exist unique sequences $\underline{u}_1$ over $\mathbf{Z}/(R)$ and $\underline{u}_2$ over $\mathbf{Z}/(Q)$ such that

$$\underline{a}\equiv Q\cdot\underline{u}_1+R\cdot\underline{u}_2 \bmod 2^{32}-1, \tag{10}$$

and moreover, it can be seen that $\underline{u}_1\in G'(f(x),R)$ and $\underline{u}_2\in G'(f(x),Q)$. Analogously, we have that

$$\underline{b}\equiv Q\cdot\underline{v}_1+R\cdot\underline{v}_2 \bmod 2^{32}-1, \tag{11}$$

where $\underline{v}_1\in G'(f(x),R)$ and $\underline{v}_2\in G'(f(x),Q)$. Since $\underline{a}\equiv\underline{b} \bmod R$, it follows that $\underline{u}_1=\underline{v}_1$, and so

$$\underline{a}-\underline{b}\equiv R\cdot\left(\underline{u}_2-\underline{v}_2\right) \bmod 2^{32}-1.$$

Furthermore, for any prime factor q of Q, since $\underline{a}\not\equiv\underline{b} \bmod q$, we have that $\underline{u}_2\not\equiv\underline{v}_2 \bmod q$, and so $\left[\underline{u}_2-\underline{v}_2\right]_{\bmod Q}\in G'(f(x),Q)$. Hence if we set

$$\underline{u}=\left[Q\cdot\underline{u}_1+R\cdot\left(\underline{u}_2-\underline{v}_2\right)\right]_{\bmod 2^{32}-1},$$

then it can be seen that $\underline{u}\in G'(f(x),2^{32}-1)$, and so by Assumption 1 we know that $\left(u_1(t),\left[u_2(t)-v_2(t)\right]_{\bmod Q}\right)$ runs through the set $\mathbf{Z}/(R)\times\mathbf{Z}/(Q)$ as t runs from 0 to $T-1$, where T is the period of $f(x)$ over $\mathbf{Z}/(2^{32}-1)$.

With the above preparations, we shall discuss the two cases $1<R<2^{16}$ and $2^{16}\le R<2^{32}-1$, respectively.

Case 1: $1<R<2^{16}$. We choose a nonnegative integer t^* such that $u_1(t^*)=0$ and

$$u_2\left(t^*\right)-v_2\left(t^*\right)\equiv 1 \bmod Q. \tag{12}$$

Then by (10) and (11) we get

$$a\left(t^*\right)=R\cdot u_2\left(t^*\right) \text{ and } b\left(t^*\right)=R\cdot v_2\left(t^*\right). \tag{13}$$

Since $a(t^*)\equiv b(t^*) \bmod h$ and $\gcd(h,R)=1$, it follows that

$$u_2\left(t^*\right)\equiv v_2\left(t^*\right) \bmod h. \tag{14}$$

Combining (12) and (14) we can deduce that

$$\begin{cases} u_2(t^*)=0,\\ v_2(t^*)=Q-1, \end{cases} \tag{15}$$

and this together with (14) implies that

$$Q \equiv 1 \bmod h. \tag{16}$$

Taking (15) into (13) yields

$$a\left(t^*\right) = 0 \text{ and } b\left(t^*\right) = 2^{32} - 1 - R.$$

Then by Lemma 2 we have that

$$a\left(t^* + T/2\right) = 0 \text{ and } b\left(t^* + T/2\right) = 2^{32} - 1 - 2^{16} \cdot R,$$

and so $\underline{a} \equiv \underline{b} \bmod h$ implies that

$$0 \equiv 2^{32} - 1 - 2^{16} \cdot R \bmod h,$$

that is,

$$Q \equiv 2^{16} \bmod h. \tag{17}$$

Then by (16) and (17) we have that $2^{16} \equiv 1 \bmod h$, which shows that h is a prime factor of $2^{16} - 1$, a contradiction to the assumption that $\gcd\left(h, 2^{32} - 1\right) = 1$.

Case 2: $2^{16} \leq R < 2^{32} - 1$. In this case, it can be seen that $2^{16} + 1$ is a prime factor of R. Therefore we assume

$$R = \left(2^{16} + 1\right) \cdot d,$$

where d is a factor of $2^{16} - 1$ with $1 \leq d < 2^{16} - 1$. We choose a nonnegative integer t^* such that $u_1\left(t^*\right) = d$ and

$$u_2\left(t^*\right) - v_2\left(t^*\right) \equiv 1 \bmod Q. \tag{18}$$

Since $Q = (2^{16} - 1)/d$ and

$$2^{16} - 1 + R \cdot k \leq 2^{16} - 1 + R \cdot (Q - 1) < 2^{32} - 1, k \in \{u_2\left(t^*\right), v_2\left(t^*\right)\},$$

by (10) and (11) we get

$$a\left(t^*\right) = 2^{16} - 1 + R \cdot u_2\left(t^*\right) \text{ and } b\left(t^*\right) = 2^{16} - 1 + R \cdot v_2\left(t^*\right). \tag{19}$$

Then $\underline{a} \equiv \underline{b} \bmod h$ implies that

$$2^{16} - 1 + R \cdot u_2\left(t^*\right) \equiv 2^{16} - 1 + R \cdot v_2\left(t^*\right) \bmod h,$$

that is,

$$u_2\left(t^*\right) \equiv v_2\left(t^*\right) \bmod h, \tag{20}$$

Combining (18) and (20) we can deduce that

$$\begin{cases} u_2\left(t^*\right) = 0, \\ v_2\left(t^*\right) = Q - 1, \end{cases} \tag{21}$$

and this together with (21) implies that

$$Q \equiv 1 \bmod h.$$

Taking (21) into (19) yields

$$a\left(t^*\right) = 2^{16} - 1 \text{ and } b\left(t^*\right) = 2^{32} + 2^{16} - 2 - R.$$

Note that

$$2^{16}R \equiv 2^{16}(2^{16}+1)d \equiv (2^{16}+1)d \equiv R \bmod 2^{32}-1,$$

and so by Lemma 2 we get

$$a\left(t^*+T/2\right) = 2^{32}-2^{16} \text{ and } b\left(t^*+T/2\right) = 2^{32}-2^{16}-R.$$

Then $\underline{a} \equiv \underline{b} \bmod h$ gives $R \equiv 0 \bmod h$, a contradiction to $\gcd\left(h, 2^{32}-1\right) = 1$.

Therefore, we have that $R = 2^{32}-1$.

(ii) It is clear that

$$per\left(\left[\underline{a}\right]_{\bmod H}\right) \le per\left(\underline{a}\right). \tag{22}$$

For any integer $k \ge 0$, let us denote by $L^k\underline{a}$ the k-shift of $\underline{a}$, i.e., $L^k\underline{a} = (a(t+k))_{t\ge 0}$. Obviously, we have that $L^k\underline{a} \in G'(f(x), 2^{32}-1)$ for all $k \ge 0$. Since

$$L^k\underline{a} \ne \underline{a} \text{ for } 0 < k < per\left(\underline{a}\right),$$

it follows from (i) that

$$L^k\underline{a} \not\equiv \underline{a} \bmod H \text{ for } 0 < k < per\left(\underline{a}\right),$$

which implies that

$$per\left(\left[\underline{a}\right]_{\bmod H}\right) \ge per\left(\underline{a}\right). \tag{23}$$

Thus (22) and (23) imply that $per\left(\left[\underline{a}\right]_{\bmod H}\right) = per\left(\underline{a}\right)$. □

4 Conclusions

Let $f(x)$ be a primitive polynomial of positive degree n over $\mathbf{Z}/(2^{32}-1)$ and H a positive integer with a prime factor coprime with $2^{32}-1$. This paper studies the distinctness of modulo H reductions of primitive sequences generated by $f(x)$ over $\mathbf{Z}/(2^{32}-1)$. In particular, the results for $H = 2$ implies that 32 2-adic coordinate sequences of a primitive sequence $\underline{a}$ over $\mathbf{Z}/(2^{32}-1)$ have similar cryptographic properties, namely every 2-adic coordinate sequence has the same period as $\underline{a}$ and uniquely determines $\underline{a}$. Primitive sequences over $\mathbf{Z}/(2^{32}-1)$ is usually compared with primitive sequences over $\mathbf{Z}/(2^{31}-1)$. The distinctness of modulo reductions of primitive sequences over $\mathbf{Z}/(2^{31}-1)$ has been completely solved for several years. With the work of this paper, now the focus of the comparison only rests on that $2^{32}-1$ is a composite number while $2^{31}-1$ is a prime number. In specific, since $2^{32}-1$ has the factorization $2^{32}-1 = 3\times 5\times 17\times 257\times 65537$, a primitive sequence $\underline{a}$ over $\mathbf{Z}/(2^{32}-1)$ can be seen as a composition of five sequences over $\mathbf{Z}/(3)$, $\mathbf{Z}/(5)$, $\mathbf{Z}/(17)$, $\mathbf{Z}/(257)$ and $\mathbf{Z}/(65537)$, respectively. So far no convincing evidence shows that this makes stream ciphers based on primitive sequences over $\mathbf{Z}/(2^{32}-1)$ more vulnerable, and this will be one of the subjects of future work.

Acknowledgements We would like to thank the anonymous reviewers for many helpful comments and suggestions. This research is supported by NSF of China under Grant No. (61070178, 61100202, 60833008).

References

1. 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).
2. Bylkov D.N., Nechaev A.A.: An algorithm to restore a linear recurring sequence over the ring $R = \mathbf{Z}_{p^n}$ from a linear complication of its highest coordinate sequence. Discr. Math. Appl. **20**(5–6), 591–609 (2010).
3. 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).
4. Dai Z.D., Beth T., Gollman D.: Lower bounds for the linear complexity of sequences over residue ring. In: Advances in Cryptology: Eurocrypt 1990. LNCS, vol. 473, pp. 189–195. Springer, Berlin (1991).
5. Dai Z.D.: Binary sequences derived from ML-sequences over rings I: periods and minimal polynomials. J. Cryptol. **5**, 193–207 (1992).
6. 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
7. Fan S.Q., Han W.B.: Random properties of the highest level sequences of primitive sequences over $\mathbf{Z}/(2^e)$. IEEE Trans. Inf. Theory **49**(6), 1553–1557 (2003).
8. Hu H.G., Feng D.G., Wu W.L.: Incomplete exponential sums over galois rings with applications to some binary sequences derived from $\mathbf{Z}/(2^l)$. IEEE Trans. Inf. Theory **52**(5), 2260–2265 (2006).
9. Huang M.Q., Dai Z.D.: Projective maps of linear recurring sequences with maximal p-adic periods. Fibonacci Q. **30**, 139–143 (1992).
10. Klimov A., Shamir A.: A new class of invertible mappings. In: Cryptographic Hardware and Embedded Systems: CHES 2002. LNCS, vol. 2523, pp. 470–483. Springer, Berlin (2003).
11. Kurakin V.L.: The first coordinate sequence of a linear recurrence of maximal period over a Galois ring. Discr. Math. Appl. **4**(2), 129–141 (1994).
12. Kuzmin A.S., Nechaev A.A.: Linear recurring sequences over Galois ring. Russ. Math. Surv. **48**, 171–172 (1993).
13. Kuzmin A.S.: Low estimates for the ranks of coordinate sequences of linear recurrent sequences over primary residue rings of integers. Russ. Math. Surv. **48**, 203–204 (1993).
14. Qi W.F., Yang J.H., Zhou J.J.: ML-sequences over rings $\mathbf{Z}/(2^e)$. In: Advances in Cryptology: Asiacrypt 1998. LNCS, vol. 1514, pp. 315–325. Springer, Berlin (1998).
15. Qi W.F., Zhu X.Y.: Compressing mappings on primitive sequences over $\mathbf{Z}/(2^e)$ and its Galois extension. Finite Fields Appl. **8**, 570–588 (2002).
16. Sole P., Zinoviev D.: The most significant bit of maximum length sequences over $\mathbf{Z}/(2^l)$: autocorrelation and imbalance. IEEE Trans. Inf. Theory **50**(8), 1844–1846 (2004).
17. Tian T., Qi W.F.: Injectivity of compressing maps on primitive sequences over $\mathbf{Z}/(p^e)$. IEEE Trans. Inf. Theory **53**(8), 2966–2970 (2007).
18. Tian T., Qi W.F.: Typical primitive polynomials over integer residue rings. Finite Fields Appl. **15**, 796–807 (2009).
19. Ward M.: The distribution of residues in a sequence satisfying a linear recursion relation. Trans. Am. Math. Soc. **33**, 166–190 (1931).
20. Ward M.: Some arithmetical properties of sequences satisfying a linear recursion relation. Ann. Math. **32**(2), 734–738 (1931).
21. Ward M.: The arithmetical theory of linear recurring series. Trans. Am. Math. Soc. **35**, 600–628 (1933).
22. Zheng Q.X., Qi W.F.: Distribution properties of compressing sequences derived from primitive sequences over $\mathbf{Z}/(p^e)$. IEEE Trans. Inf. Theory **56**(1), 555–563 (2010).
23. 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).
24. Zheng Q.X., Qi W.F., Tian T.: On the distinctness of binary sequences derived from primitive sequences modulo square-free odd integers, summitted to IEEE Trans. Inf. Theory. Available at: http://www.eprint.iacr.org/2012/003.pdf
25. Zhu X.Y., Qi W.F.: Compression mappings on primitive sequences over $\mathbf{Z}/(p^e)$. IEEE Trans. Inf. Theory **50** (10), 2442–2448 (2004).
26. Zhu X.Y., Qi W.F.: Further result of compressing maps on primitive sequences modulo odd prime powers. IEEE Trans. Inf. Theory **53**(8), 2985–2990 (2007).
27. Zhu X.Y., Qi W.F.: On the distinctness of modular reductions of maximal length sequences modulo odd prime powers. Math. Comp. **77**(7), 1623–1637 (2008).