On the distinctness of binary sequences derived from primitive sequences modulo square-free odd integers[*]

Qun-Xiong Zheng, Wen-Feng Qi and Tian Tian[†]

August 21, 2011

Abstract

Let M be a square-free odd integer and $\mathbf{Z}/(M)$ the integer residue ring modulo M. This paper studies the distinctness of primitive sequences over $\mathbf{Z}/(M)$ modulo 2. Recently, for the case of $M = pq$, a product of two distinct prime numbers p and q, the problem has been almost completely solved. As for the case that M is a product of more prime numbers, the problem has been quite resistant to proof. In this paper, a partial proof is given by showing that a class of primitive sequences of order $2k+1$ over $\mathbf{Z}/(M)$ is distinct modulo 2. Besides as an independent interest, the paper also involves two distribution properties of primitive sequences over $\mathbf{Z}/(M)$, which related closely to our main results.

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, Wen-Feng Qi and Tian Tian are with the department of Applied Mathematics, Zhengzhou Information Science and Technology Institute, Zhengzhou 450002, China. (e-mail: qunxiong_-zheng@163.com, wenfeng.qi@263.net and tiantian_d@126.com)

1 Introduction

Let $\mathbf{Z}/(M)$ denote the integer residue ring modulo M for any integer $M \geq 2$. If a sequence $\underline{a} = (a(t))_{t\geq 0}$ over $\mathbf{Z}/(M)$ satisfies

$$a(i+n) \equiv -\left(c_{n-1}a(i+n-1) + \cdots + c_1 a(i+1) + c_0 a(i)\right) \bmod M, \ i \geq 0 \qquad (1)$$

with constant coefficients $c_0, c_1, \ldots, c_{n-1} \in \mathbf{Z}/(M)$, then $\underline{a}$ is called a linear recurring sequence of order n over $\mathbf{Z}/(M)$ generated by $f(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_0$ (or $\underline{a}$ is a sequence of order n over $\mathbf{Z}/(M)$ in short) and $f(x)$ is called a characteristic polynomial of $\underline{a}$. For convenience, the set of sequences generated by $f(x)$ over $\mathbf{Z}/(M)$ is generally denoted by $G(f(x), M)$.

Let p be a prime number and e a positive integer. 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 $\mathbf{Z}/(p^e)$, 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** of order n if $\underline{a}$ is generated by a primitive polynomial of degree n over $\mathbf{Z}/(p^e)$ and $\underline{a} \bmod p = (a(t) \bmod p)_{t\geq 0}$ is not an all 0 sequence. The period of a primitive sequence $\underline{a}$ of order n over $\mathbf{Z}/(p^e)$, denoted as $per(\underline{a}, p^e)$, is equal to $p^{e-1}(p^n-1)$, see [1].

Every element $u \in \mathbf{Z}/(p^e)$ has a unique p-adic expansion as $u = u_0 + u_1 \cdot p + \cdots + u_{e-1} \cdot p^{e-1}$, where $u_i \in \{0, 1, \ldots, p-1\}$ 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 $\underline{a} = \underline{a}_0 + \underline{a}_1 \cdot p + \cdots + \underline{a}_{e-1} \cdot p^{e-1}$, where $\underline{a}_i$ is a sequence over $\{0, 1, \ldots, p-1\}$ and can be naturally seen as a sequence over $\mathbf{Z}/(p)$. The sequence $\underline{a}_i$ 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 $\underline{a}$.

Let $\underline{a}$ be a sequence over $\mathbf{Z}/(p^e)$ with the p-adic expansion as $\underline{a} = \underline{a}_0 + \underline{a}_1 \cdot p + \cdots + \underline{a}_{e-1} \cdot p^{e-1}$ and $\varphi(x_0, \ldots, x_{e-1})$ an e-variable function over $\mathbf{Z}/(p)$. Then

$$\varphi(\underline{a}_0, \ldots, \underline{a}_{e-1}) = \left(\varphi(a_0(t), \ldots, a_{e-1}(t))\right)_{t\geq 0}$$

is a sequence over $\mathbf{Z}/(p)$ and is called a compressing sequence derived from $\underline{a}$. When $\underline{a}$ is a primitive sequence over $\mathbf{Z}/(p^e)$, many cryptographical properties of such compressing sequence have been studied during the last 20 years [2]-[17], in particular the distinctness of compressing sequences, 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 a 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 primitive sequences and their compressing sequences, which implies that every compressing sequence preserves all the information of its original primitive sequence. 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 $\mathbf{Z}/(p^e)$, was 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 [20], are in fact modulo 2 reductions of primitive sequences of order 1 over $\mathbf{Z}/(p^e)$. In [19], 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 $\underline{a} \equiv \underline{b} \bmod m$, where m is a positive integer with 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.

Let M be an integer greater than 1 and $M = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ the canonical factorization of M. As a natural generalization of the definitions of primitive polynomials and primitive sequences over $\mathbf{Z}/(p^e)$, a monic polynomial $f\,(x)$ of degree n over $\mathbf{Z}/(M)$ is called a **primitive polynomial** and a sequence $\underline{a} = (a(t))_{t \geq 0}$ of order n over $\mathbf{Z}/(M)$ is called a **primitive sequence**, if for every $i \in \{1, 2, \ldots, r\}$, $f\,(x) \bmod p_i^{e_i}$ is a primitive polynomial of degree n over $\mathbf{Z}/(p_i^{e_i})$ and $\underline{a} \bmod p_i^{e_i}$ is a primitive sequence of order n over $\mathbf{Z}/(p_i^{e_i})$, respectively. It is easy to see that the period of a primitive polynomial of degree n over $\mathbf{Z}/(M)$ and that of a primitive sequence of order n over $\mathbf{Z}/(M)$ are both equal to

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

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

If M has at least two different prime factors, there indeed exist many primitive sequences of order 1 over $\mathbf{Z}/(M)$ such that their modular reductions are the same [21]. It is long not clear, however, whether the modular reductions of primitive sequences of order $n \geq 2$ over $\mathbf{Z}/(M)$ are distinct. Let p and q be two distinct prime numbers. In [21], the authors first studied the distinctness of primitive sequences over $\mathbf{Z}/(pq)$ modulo 2, and a sufficient condition was given for (n, p, q) such that primitive sequences of order n over $\mathbf{Z}/(pq)$ are distinct modulo 2. Then in [18] based on a new result on the element distribution property of primitive sequences over $\mathbf{Z}/(pq)$, the set of primitive sequences that can be proved to be distinct modulo 2 is greatly enlarged and almost includes all primitive sequences.

Inspired by the methods of [18], this paper studies a much more general modulus M which is a product of three or more distinct prime numbers. A class of primitive sequences of order $n = 2k+1$ over $\mathbf{Z}/(M)$ is shown to be distinct modulo 2, where $k \geq 1$ is an integer. The number of primitive sequences proved to be distinct modulo 2 has close relations with two distribution properties of primitive sequences over $\mathbf{Z}/(M)$. One is given $s \in \mathbf{Z}/(M)$ and a primitive sequence $\underline{a}$ of order $n \geq 2$ over $\mathbf{Z}/(M)$ whether there is an integer $t \geq 0$ such that $a(t) = s$. The other is given a primitive sequence $\underline{a}$ of order 1 over $\mathbf{Z}/(M)$ whether there is an integer $t \geq 0$ such that $a(t)$ is an even number. Based on the estimates of exponential sums over integer residue rings and number theoretical functions, sufficient conditions of primitive sequences over $\mathbf{Z}/(M)$ satisfying the two properties are obtained, respectively, and corresponding experimental data are provided to show the validity of the sufficient conditions.

The paper is organized as follows. Section 2 presents some necessary preliminaries. Section 3 discusses distribution properties of primitive sequences over integer residue rings.

Section 4 is largely devoted to the proof of our main result. Finally, conclusions are drawn in Section 5.

Throughout the paper, we assume that M is a square-free odd integer and $M = p_1p_2\cdots p_r$ is the canonical factorization of M, where $r \geq 2$ and p_i is an odd prime number for $1 \leq i \leq r$. We choose $\{0, 1, \ldots, M-1\}$ as the complete set of representatives for the elements of the ring $\mathbf{Z}/(M)$. Thus a sequence $\underline{a}$ over $\mathbf{Z}/(M)$ is usually seen as an integer sequence over $\{0, 1, \ldots, M-1\}$. Moreover, for an integer x and a positive integer m, we denote the nonnegative minimal residue of x modulo m as $[x]_{\bmod m}$ and $[\underline{a}]_{\bmod m} = ([a(t)]_{\bmod m})_{t\geq 0}$ for a sequence $\underline{a} = (a(t))_{t\geq 0}$ over $\mathbf{Z}/(M)$.

2 Preliminaries

An element $\xi \in \mathbf{Z}/(M)$ is called a primitive element of $\mathbf{Z}/(M)$ if $[\xi]_{\bmod p_i}$ is a primitive element of $\mathbf{Z}/(p_i)$ for every $i \in \{1, 2, \ldots, r\}$, i.e., the multiplicative order of $[\xi]_{\bmod p_i}$ in $\mathbf{Z}/(p_i)$ is equal to $p_i - 1$. It can be seen that the multiplicative order of any primitive element in $\mathbf{Z}/(M)$ is equal to $\operatorname{lcm}(p_1 - 1, p_2 - 1, \ldots, p_r - 1)$.

Typical primitive polynomials over integer residue rings were first proposed and studied in [22]. The authors of [22] gave the following equivalent conditions, each of which defines a typical primitive polynomial.

Lemma 1 *([22]) Let $f(x)$ be a primitive polynomial of degree n over $\mathbf{Z}/(M)$. Then the following are equivalent:*

(1) $f(x)$ divides $x^S - \xi$ for some positive integer S and some primitive element ξ of $\mathbf{Z}/(M)$;

(2) there exists a primitive element ξ of $\mathbf{Z}/(M)$ such that $x^{\theta_M} \equiv \xi \bmod f(x)$ holds over $\mathbf{Z}/(M)$, where $\theta_M = \operatorname{lcm}\left(\frac{p_1^n-1}{p_1-1}, \frac{p_2^n-1}{p_2-1}, \ldots, \frac{p_r^n-1}{p_r-1}\right)$;

(3) $\gcd\left(\theta_{p_ip_j}, p_i^n - 1\right) = \frac{p_i^n-1}{p_i-1}$ *for any pair of distinct prime divisors* p_i *and* p_j *of* M*, where* $\theta_{p_ip_j} = \operatorname{lcm}\left(\frac{p_i^n-1}{p_i-1}, \frac{p_j^n-1}{p_j-1}\right)$.

Remark 2 *The conditions (1), (2) and (3) correspond to Definition 4 , Lemma 5 and formula (9) of [22], respectively.*

Definition 3 *([22]) A monic polynomial* $f(x)$ *of degree* n *over* $\mathbf{Z}/(M)$ *is called a typical primitive polynomial of degree* n *over* $\mathbf{Z}/(M)$ *if* $f(x)$ *is primitive and satisfies the equivalent conditions of Lemma 1.*

It can be seen from the condition (3) of Lemma 1 that the existence of typical primitive polynomials of degree n over $\mathbf{Z}/(M)$ only depends on the arithmetic properties of M and n. Thus, for convenience we call (M, n) a typical primitive pair if M and n satisfy the condition (3) of Lemma 1.

To prove the distinctness of primitive sequences over $\mathbf{Z}/(M)$ modulo 2 in Section 4, we need another concept named "a distinguishable pair", and we make its definition explicit in the following statement.

Definition 4 *Let* n *be a positive integer. Then* (M, n) *is called a distinguishable pair if*

$$\gcd\left(\frac{p_i^n - 1}{p_i - 1}, p_j^n - 1\right) = 1 \tag{2}$$

for any pair of distinct prime divisors p_i *and* p_j *of* M*.*

Remark 5 (1) *If* (M, n) *is a distinguishable pair, then it is necessary that* n *is an odd number. This is because if* n *is an even number, then both* $\frac{p_i^n-1}{p_i-1} = \sum_{k=0}^{n-1} p_i^k$ *and* $p_j^n - 1$ *are even numbers, and so* $\gcd\left(\frac{p_i^n-1}{p_i-1}, p_j^n - 1\right) \geq 2 \neq 1$.

(2) *If* (M, n) *is a distinguishable pair, then* (M, n) *is a typical primitive pair, but the reverse is not true. For example, it can be verified that* $(77, 3)$ *is a typical primitive pair, but not a distinguishable pair.*

(3) *Experimental data show that the proportion of distinguishable pairs* (M, n) *is about* 61.148% *when* M *runs through all possible values between* 1 *and* $10,000,000$ *and* n *runs through all odd integers between* 3 *and* 19.

Finally we recall the estimates of some classical exponential sums over integer residue rings. Let m be a positive integer greater than 1, and let $e_m(\cdot)$ be the canonical additive character over $\mathbf{Z}/(m)$ given by $e_m(a) = e^{2\pi i a/m}$, where a is an integer. First it is well-known that the complete sum

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

for any integer c. Second the following estimates are proved in [23].

Lemma 6 *[23, Lemma 8.80] For any positive integer* H *we have*

$$\sum_{a=0}^{m-1} \left| \sum_{x=0}^{H-1} e_m(ax) \right| < 2m \left(\frac{\ln m}{\pi} + \frac{1}{5} \right) + H,$$

where $\ln(\cdot)$ *is the natural logarithm. In particular, we have*

$$\sum_{a=1}^{m-1} \left| \sum_{x=0}^{H-1} e_m(ax) \right| < 2m \left(\frac{\ln m}{\pi} + \frac{1}{5} \right).$$

3 Distribution Properties of Primitive Sequences over $\mathbf{Z}/(M)$

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

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

In this section, we discuss two distribution problems of primitive sequences over $\mathbf{Z}/(M)$, which will be shown to be useful in Section 4. The first problem is whether every element of $\mathbf{Z}/(M)$ occurs in a complete period of a primitive sequence of order n over $\mathbf{Z}/(M)$. In Subsection 3.1, we shall show that the answer is positive for sufficiently large n. It is clear that the answer is negative for $n = 1$. The second problem is whether there exists an even number of $\mathbf{Z}/(M)$ occurs in a complete period of a primitive sequence of order 1 over $\mathbf{Z}/(M)$. In Subsection 3.2, we shall show that the answer to this problem is positive for almost all M's. The main results of this section are based on the estimates of exponential sums over integer residue rings.

3.1 Estimates for the number of a given element occurring in a primitive sequence over $\mathbf{Z}/(M)$

Lemma 7 *Let $f(x) = x^n - (c_{n-1}x^{n-1} + \cdots + c_1x + c_0)$ be a primitive polynomial over $\mathbf{Z}/(M)$ with period T and $\mathbf{d} = (1, 0, \ldots, 0) \in (\mathbf{Z}/(M))^n$. Then $\mathbf{d} \cdot A^h \neq \mathbf{d} \cdot A^k$ for $0 \leq h < k < T$, where*

$$A = \begin{bmatrix} 0 & 1 & 0 & 0 & \cdots & 0 \\ 0 & 0 & 1 & 0 & \cdots & 0 \\ 0 & 0 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \cdots & 1 \\ c_0 & c_1 & c_2 & c_3 & \cdots & c_{n-1} \end{bmatrix}. \tag{3}$$

(Here we mean that $A = [c_0]$ if $n = 1$.)

Proof. Suppose there exist two integers h and k, $0 \leq h < k < T$, such that $\mathbf{d} \cdot A^h = \mathbf{d} \cdot A^k$. Then we have

$$\left(\mathbf{d} \cdot A^j\right) \cdot A^h = \left(\mathbf{d} \cdot A^j\right) \cdot A^k \text{ for } 0 \leq j \leq n-1. \tag{4}$$

Note that

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

and so (4) implies that

$$A^h = A^k. \tag{5}$$

Let $\underline{d} = (d(t))_{t \geq 0}$ be a primitive sequence generated by $f(x)$ over $\mathbf{Z}/(M)$, and let

$$\mathbf{d}_t = (d(t), d(t+1), \ldots, d(t+n-1))$$

be the t-th state of the sequence $\underline{d}$ for any integer $t \geq 0$. It follows from (1) that

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

where $\mathbf{d}_t^\tau$ is the transpose of $\mathbf{d}_t$. Then by (5) we have

$$\mathbf{d}_h^\tau = A^h \cdot \mathbf{d}_0^\tau = A^k \cdot \mathbf{d}_0^\tau = \mathbf{d}_k^\tau,$$

and so the period of $\underline{d}$ is not greater than $k - h < T$, a contradiction to the fact that the period of $\underline{d}$ is equal to T. Therefore we get that $\mathbf{d} \cdot A^h \neq \mathbf{d} \cdot A^k$ for $0 \leq h < k < T$. ■

The following lemma is an analogy of Theorem 8.78 of [23].

Lemma 8 *Let $\underline{a}$ be a primitive sequence of order n over $\mathbf{Z}/(M)$ with period*

$$T = \operatorname{lcm}(p_1^n - 1, p_2^n - 1, \ldots, p_r^n - 1).$$

Then

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

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

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

Note that

$$\begin{aligned} & e_M\left(b_0 a(0)+b_1 a(1)+\cdots+b_{n-1} a(n-1)\right) \\ = & e_M\left(b_0 a(T)+b_1 a(T+1)+\cdots+b_{n-1} a(T+n-1)\right), \end{aligned}$$

and so we obtain

$$\sigma(\mathbf{b})=\sum_{t=0}^{T-1} e_M\left(b_0 a(t+1)+b_1 a(t+2)+\cdots+b_{n-1} a(t+n)\right). \tag{7}$$

Assume $f(x)=x^n-\left(c_{n-1} x^{n-1}+\cdots+c_1 x+c_0\right)$ is a characteristic polynomial of $\underline{a}$. Then we have

$$a(t+n) \equiv c_0 a(t)+c_1 a(t+1)+\cdots+c_{n-1} a(t+n-1) \bmod M, t \geq 0. \tag{8}$$

Hence, (7) and (8) yield

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

where A is an $n \times n$ matrix over $\mathbf{Z}/(M)$ of the form described in (3). Recursively, we have

$$|\sigma(\mathbf{b})|=|\sigma(\mathbf{b} \cdot A)|=\left|\sigma\left(\mathbf{b} \cdot A^2\right)\right|=\cdots=\left|\sigma\left(\mathbf{b} \cdot A^{T-1}\right)\right|. \tag{9}$$

Let $\mathbf{d}=(1,0, \ldots, 0) \in(\mathbf{Z}/(M))^n$ and $\Omega=\left\{\mathbf{d} \cdot A^t \mid 0 \leq t \leq T-1\right\}$. On one hand, it can be seen from (6) that

$$T \cdot\left|\sum_{t=0}^{T-1} e_M(a(t))\right|^2=T \cdot|\sigma(\mathbf{d})|^2. \tag{10}$$

On the other hand, since Lemma 7 implies that the number of elements in Ω equals T, it follows from (9) that

$$T \cdot|\sigma(\mathbf{d})|^2=\sum_{t=0}^{T-1}\left|\sigma\left(\mathbf{d} A^t\right)\right|^2=\sum_{\mathbf{b} \in \Omega}|\sigma(\mathbf{b})|^2 \leq \sum_{\mathbf{b} \in(\mathbf{Z}/(M))^n}|\sigma(\mathbf{b})|^2. \tag{11}$$

Thus, (10) and (11) yield

$$T \cdot \left| \sum_{t=0}^{T-1} e_M\left(a\left(t\right)\right) \right|^2 \leq \sum_{\mathbf{b} \in (\mathbf{Z}/(M))^n} \left|\sigma\left(\mathbf{b}\right)\right|^2 . \tag{12}$$

Note that

$$\begin{aligned} \sum_{\mathbf{b} \in (\mathbf{Z}/(M))^n} \left|\sigma\left(\mathbf{b}\right)\right|^2 &= \sum_{\mathbf{b} \in (\mathbf{Z}/(M))^n} \sigma\left(\mathbf{b}\right) \cdot \overline{\sigma\left(\mathbf{b}\right)} \\ &= \sum_{0 \leq s,t \leq T-1} \left(\sum_{b_0 \in \mathbf{Z}/(M)} e_M\left(b_0\left(a\left(s\right) - a\left(t\right)\right)\right) \right) \cdot \cdots \\ &\quad \cdot \left(\sum_{b_{n-1} \in \mathbf{Z}/(M)} e_M\left(b_{n-1}\left(a\left(s+n-1\right) - a\left(t+n-1\right)\right)\right) \right) . \end{aligned} \tag{13}$$

Since

$$\left(a\left(s\right), \ldots, a\left(s+n-1\right)\right) = \left(a\left(t\right), \ldots, a\left(t+n-1\right)\right) \text{ if and only if } s \equiv t \bmod T,$$

it follows from (13) that

$$\sum_{\mathbf{b} \in (\mathbf{Z}/(M))^n} \left|\sigma\left(\mathbf{b}\right)\right|^2 = T \cdot M^n. \tag{14}$$

Finally combining (12) and (14), we get

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

■

Remark 9 *Note that r is assumed to be greater than 1. But Theorem 8.78 of [23] implies that Lemma 8 is also true if $r = 1$.*

Lemma 10 *Let p be a prime number and $\underline{a}$ a primitive sequence of order n over $\mathbf{Z}/(p)$. Then for any integer s we have*

$$E_p(s) = \sum_{t=0}^{p^n-2} \sum_{h=0}^{p-1} e_p\left(h \cdot \left(a\left(t\right) - s\right)\right) = \begin{cases} p^n - p, & \text{if } s \equiv 0 \bmod p; \\ p^n, & \text{if } \gcd(s,p) = 1. \end{cases} \tag{15}$$

Proof. Since the exponential sum

$$\frac{1}{p}\cdot\sum_{t=0}^{p^n-2}\sum_{h=0}^{p-1}e_p\left(h\cdot\left(a\left(t\right)-s\right)\right)$$

counts the number of the element $s \bmod p$ occurring in a complete period of $\underline{a}$, (15) immediately follows from the element distribution properties of m-sequences over finite fields. ■

Let $\underline{a}$ be a primitive sequence of order n over $\mathbf{Z}/(M)$, and let

$$T=per(\underline{a},M)=\mathrm{lcm}(p_1^n-1,p_2^n-1,\ldots,p_r^n-1).$$

Given an element $s\in\mathbf{Z}/(M)$, it can be seen that

$$N\left(\underline{a}^T,s\right)=\frac{1}{M}\sum_{t=0}^{T-1}\left(\sum_{h_1=0}^{p_1-1}e_{p_1}\left(h_1\cdot\left(a\left(t\right)-s\right)\right)\cdots\sum_{h_r=0}^{p_r-1}e_{p_r}\left(h_r\cdot\left(a\left(t\right)-s\right)\right)\right).$$

For $i=1,2,\ldots,r$, let us denote

$$D_i=\sum_{h_i=1}^{p_i-1}e_{p_i}\left(h_i\cdot\left(a\left(t\right)-s\right)\right).$$

Then

$$\begin{aligned}N\left(\underline{a}^T,s\right) &= \frac{1}{M}\sum_{t=0}^{T-1}\prod_{i=1}^{r}(D_i+1)\\ &= \frac{1}{M}\sum_{t=0}^{T-1}\left(1+\sum_{i=1}^{r}D_i+\sum_{k=2}^{r}\sum_{1\le i_1<\cdots<i_k\le r}D_{i_1}D_{i_2}\cdots D_{i_k}\right)\\ &= \frac{T}{M}+\frac{1}{M}\sum_{i=1}^{r}\sum_{t=0}^{T-1}D_i+\frac{1}{M}\sum_{t=0}^{T-1}\sum_{k=2}^{r}\sum_{1\le i_1<\cdots<i_k\le r}D_{i_1}D_{i_2}\cdots D_{i_k}. \qquad (16)\end{aligned}$$

Note that for $i=1,2,\ldots,r$, we have that

$$\begin{aligned}\sum_{t=0}^{T-1}D_i &= \sum_{t=0}^{T-1}\sum_{h_i=1}^{p_i-1}e_{p_i}\left(h_i\cdot\left(a\left(t\right)-s\right)\right)\\ &= \sum_{t=0}^{T-1}\sum_{h_i=0}^{p_i-1}e_{p_i}\left(h_i\cdot\left(a\left(t\right)-s\right)\right)-T\\ &= \frac{T}{p_i^n-1}\sum_{t=0}^{p_i^n-2}\sum_{h_i=0}^{p_i-1}e_{p_i}\left(h_i\cdot\left(a\left(t\right)-s\right)\right)-T.\end{aligned}$$

It follows from Lemma 10 that

$$\sum_{t=0}^{T-1} D_i = \frac{T \cdot E_{p_i}(s)}{p_i^n - 1} - T, i = 1, 2, \ldots, r. \tag{17}$$

Taking (17) into (16) yields

$$\begin{aligned} & \left| N\left(\underline{a}^T, s\right) - \frac{T}{M}\left(1 - r + \sum_{i=1}^{r} \frac{E_{p_i}(s)}{p_i^n - 1}\right) \right| \\ = \;& \frac{1}{M} \left| \sum_{k=2}^{r} \sum_{1 \le i_1 < \cdots < i_k \le r} \sum_{t=0}^{T-1} D_{i_1} D_{i_2} \cdots D_{i_k} \right| \\ \le \;& \frac{1}{M} \sum_{k=2}^{r} \sum_{1 \le i_1 < \cdots < i_k \le r} \sum_{h_{i_1}=1}^{p_{i_1}-1} \cdots \sum_{h_{i_k}=1}^{p_{i_k}-1} \left| \sum_{t=0}^{T-1} e_{p_{i_1}}\left(h_{i_1}\left(a\left(t\right) - s\right)\right) \cdots e_{p_{i_k}}\left(h_{i_k}\left(a\left(t\right) - s\right)\right) \right| \\ = \;& \frac{1}{M} \sum_{k=2}^{r} \sum_{1 \le i_1 < \cdots < i_k \le r} \sum_{h_{i_1}=1}^{p_{i_1}-1} \cdots \sum_{h_{i_k}=1}^{p_{i_k}-1} \left| \sum_{t=0}^{T-1} e_{p_{i_1}}\left(h_{i_1} a\left(t\right)\right) \cdots e_{p_{i_k}}\left(h_{i_k} a\left(t\right)\right) \right|. \end{aligned} \tag{18}$$

For given $1 \le i_1 < i_2 < \cdots < i_k \le r$, set

$$g_{i_d} = \frac{\prod_{1 \le j \le k} p_{i_j}}{p_{i_d}}, d = 1, 2, \ldots, k.$$

Then it can be seen that

$$e_{p_{i_1}}\left(h_{i_1} a\left(t\right)\right) e_{p_{i_2}}\left(h_{i_2} a\left(t\right)\right) \cdots e_{p_{i_k}}\left(h_{i_k} a\left(t\right)\right) = e_{p_{i_1} p_{i_2} \cdots p_{i_k}}((\sum_{d=1}^{k} g_{i_d} h_{i_d}) \cdot a\left(t\right)).$$

Since

$$\sum_{d=1}^{k} g_{i_d} h_{i_d} \not\equiv 0 \bmod p_{i_j}, 1 \le j \le k,$$

the sequence

$$(\sum_{d=1}^{k} g_{i_d} h_{i_d}) \cdot \underline{a} = ((\sum_{d=1}^{k} g_{i_d} h_{i_d}) \cdot a\left(t\right))_{t \ge 0}$$

is a primitive sequence over $\mathbf{Z}/(p_{i_1} p_{i_2} \cdots p_{i_k})$ with period $\operatorname{lcm}\left(p_{i_1}^n - 1, p_{i_2}^n - 1, \ldots, p_{i_k}^n - 1\right)$. Then by Lemma 8 we have

$$\left| \sum_{t=0}^{T-1} e_{p_{i_1}}\left(h_{i_1} a\left(t\right)\right) e_{p_{i_2}}\left(h_{i_2} a\left(t\right)\right) \cdots e_{p_{i_k}}\left(h_{i_k} a\left(t\right)\right) \right| \le \frac{T \cdot \left(p_{i_1} p_{i_2} \cdots p_{i_k}\right)^{n/2}}{\operatorname{lcm}\left(p_{i_1}^n - 1, p_{i_2}^n - 1, \ldots, p_{i_k}^n - 1\right)} \tag{19}$$

for all $1 \le h_{i_d} \le p_{i_d} - 1$, $1 \le d \le k$. Combining (18) and (19) yields

$$\begin{aligned}
&\left| N\left(\underline{a}^T, s\right) - \frac{T}{M} \cdot \left(1 - r + \sum_{i=1}^{r} \frac{E_{p_i}(s)}{p_i^n - 1}\right) \right| \\
\le\ & \frac{T}{M} \cdot \sum_{k=2}^{r} \sum_{1 \le i_1 < \cdots < i_k \le r} \frac{\prod_{j=1}^{k} \left(p_{i_j} - 1\right) p_{i_j}^{n/2}}{\operatorname{lcm}\left(p_{i_1}^n - 1, p_{i_2}^n - 1, \ldots, p_{i_k}^n - 1\right)}.
\end{aligned}$$

Therefore, it is clear that $N\left(\underline{a}^T, s\right) > 0$ if

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

This leads to the following theorem.

Theorem 11 *Let $\underline{a}$ be a primitive sequence of order n over $\mathbf{Z}/(M)$. For a given element $s \in \mathbf{Z}/(M)$, the element s occurs in the sequence $\underline{a}$ if*

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

In particular, every invertible element in $\mathbf{Z}/(M)$ occurs in the sequence $\underline{a}$ if

$$1 + \sum_{i=1}^{r} \frac{1}{p_i^n - 1} > \sum_{k=2}^{r} \sum_{1 \le i_1 < \cdots < i_k \le r} \frac{\prod_{j=1}^{k}(p_{i_j} - 1) p_{i_j}^{n/2}}{\operatorname{lcm}\left(p_{i_1}^n - 1, p_{i_2}^n - 1, \ldots, p_{i_k}^n - 1\right)}, \tag{20}$$

and every element in $\mathbf{Z}/(M)$ occurs in the sequence $\underline{a}$ if

$$1 - \sum_{i=1}^{r} \frac{p_i - 1}{p_i^n - 1} > \sum_{k=2}^{r} \sum_{1 \le i_1 < \cdots < i_k \le r} \frac{\prod_{j=1}^{k}(p_{i_j} - 1) p_{i_j}^{n/2}}{\operatorname{lcm}\left(p_{i_1}^n - 1, p_{i_2}^n - 1, \ldots, p_{i_k}^n - 1\right)}. \tag{21}$$

Remark 12 *It is trivial that (21) is not true for $n = 1$. Next we shall show that (21) is not true for $n = 2$ either. Since $p_i^2 \equiv 1 \bmod 4$ for all $1 \le i \le r$, it can be seen that*

$$\operatorname{lcm}\left(p_1^2 - 1, p_2^2 - 1, \ldots, p_r^2 - 1\right) \le \frac{\prod_{i=1}^{r}(p_i^2 - 1)}{4^{r-1}} \le \frac{\prod_{i=1}^{r}(p_i^2 - 1)}{2^r}.$$

Thus we have

$$\begin{aligned}
& \sum_{k=2}^{r} \sum_{1\le i_1<\cdots<i_k\le r} \frac{\prod_{j=1}^{k}(p_{i_j}-1)p_{i_j}}{\operatorname{lcm}\left(p_{i_1}^2-1, p_{i_2}^2-1, \ldots, p_{i_k}^2-1\right)} \\
\geq\ & \frac{\prod_{i=1}^{r}\left(p_i-1\right)p_i}{\operatorname{lcm}\left(p_1^2-1, p_2^2-1, \ldots, p_r^2-1\right)} \\
\geq\ & 2^r \cdot \prod_{i=1}^{r} \frac{p_i}{p_i+1} \\
>\ & 1 \\
>\ & 1-\sum_{i=1}^{r} \frac{p_i-1}{p_i^2-1}.
\end{aligned}$$

This shows that (21) is not true for $n = 2$.

Table 1 The proportions of M's satisfy (21) of Theorem 11

n	$\Omega_{1000000}$	$\Omega_{5000000}$	$\Omega_{10000000}$		n	$\Omega_{1000000}$	$\Omega_{5000000}$	$\Omega_{10000000}$
3	76.347%	76.669%	76.811%		12	99.999%	99.999%	99.999%
4	67.918%	69.891%	70.482%		13	100%	100%	100%
5	99.998%	99.998%	99.998%		14	100%	100%	100%
6	95.964%	96.164%	96.204%		15	100%	100%	100%
7	100%	100%	100%		16	100%	100%	100%
8	100%	100%	100%		17	100%	100%	100%
9	100%	100%	100%		18	100%	100%	100%
10	100%	100%	100%		19	100%	100%	100%
11	100%	100%	100%		20	100%	100%	100%

To show the validity of Theorem 11, we did some experiments on the proportions of M's satisfying (21) of Theorem 11 and we list our results in Table 1 where the notation Ω_k denotes the range of M, $k \in \{1000000, 5000000, 10000000\}$. For example, if $n = 3$, then the proportion of M's satisfying (21) of all possible values M between 1 and 1000000 is 76.347%. It can be seen from Table 1 that for $n > 6$, the proportions of M's satisfying (21) of Theorem 11 are close to 100%. In theory, the best result we can prove is that (21) holds provided n is sufficiently large.

Theorem 13 *For each square-free odd integer M, there exists an integer N_M such that (21) holds if $n > N_M$. Therefore, if $\underline{a}$ is a primitive sequence of order $n > N_M$ over $\mathbf{Z}/(M)$, then every element of $\mathbf{Z}/(M)$ occurs in the sequence $\underline{a}$.*

Proof. See Appendix A. ■

3.2 Estimates for the number of even numbers occurring in a primitive sequence of order 1 over $\mathbf{Z}/(M)$

The *Carmichael's λ-function* (denote as "$\lambda(\cdot)$") [25] will be frequently used in this subsection, and so we first make its definition explicit here. The *Carmichael's λ-function* of m is defined as the universal exponent for the group of residues modulo m that are coprime to m, i.e.,

$$\lambda(m) = \mathrm{lcm}(q_1^{e_1-1}(q_1-1), q_2^{e_2-1}(q_2-1), \ldots, q_v^{e_v-1}(q_v-1))$$

if $m = q_1^{e_1} q_2^{e_2} \cdots q_v^{e_v}$ is the canonical factorization of m. In particular, since $M = p_1 p_2 \cdots p_r$, we have $\lambda(M) = \mathrm{lcm}(p_1 - 1, p_2 - 1, \ldots, p_r - 1)$, which is equal to the period of primitive sequence of order 1 over $\mathbf{Z}/(M)$.

Lemma 14 *Let $\underline{a}$ be a primitive sequence of order 1 over $\mathbf{Z}/(M)$ with period $T = \lambda(M)$. Set $\underline{v} = [\underline{a}]_{\mathrm{mod}\,2}$. Then for $s \in \{0, 1\}$ we have*

$$\left| N\left(\underline{v}^T, s\right) - \frac{T \cdot (H_s + 1)}{M} \right| < \frac{2T}{M} \sum_{\substack{d|M \\ d>1}} \frac{d^{3/2}}{\lambda(d)} \cdot \left(\frac{\ln d}{\pi} + \frac{1}{5} \right),$$

where $H_s = \frac{M-1}{2} - s$.

Proof. Since

$$\begin{aligned} N\left(\underline{v}^T, s\right) &= \sum_{t=0}^{T-1}\sum_{x=0}^{H_s}\left(\frac{1}{M}\sum_{h=0}^{M-1} e_M\left(h\left(a\left(t\right)-2x-s\right)\right)\right) \\ &= \frac{1}{M}\sum_{h=0}^{M-1}\left(e_M\left(-hs\right)\cdot\sum_{t=0}^{T-1} e_M\left(ha\left(t\right)\right)\cdot\sum_{x=0}^{H_s} e_M\left(-2hx\right)\right) \\ &= \frac{T\cdot\left(H_s+1\right)}{M}+\frac{1}{M}\sum_{h=1}^{M-1}\left(e_M\left(-hs\right)\cdot\sum_{t=0}^{T-1} e_M\left(ha\left(t\right)\right)\cdot\sum_{x=0}^{H_s} e_M\left(-2hx\right)\right), \end{aligned}$$

it follows that

$$\begin{aligned} &\left|N\left(\underline{v}^T, s\right)-\frac{T\cdot\left(H_s+1\right)}{M}\right| \\ \leq\ & \frac{1}{M}\sum_{h=1}^{M-1}\left|\sum_{t=0}^{T-1} e_M\left(ha\left(t\right)\right)\right|\cdot\left|\sum_{x=0}^{H_s} e_M\left(-2hx\right)\right| \\ =\ & \frac{1}{M}\sum_{\substack{d\mid M\\ d>1}}\ \sum_{\substack{1\leq h\leq M-1\\ \gcd(h,M)=M/d}}\left|\sum_{t=0}^{T-1} e_M\left(ha\left(t\right)\right)\right|\cdot\left|\sum_{x=0}^{H_s} e_M\left(-2hx\right)\right| \\ =\ & \frac{1}{M}\sum_{\substack{d\mid M\\ d>1}}\ \sum_{\substack{1\leq h\leq d-1\\ \gcd(h,d)=1}}\left|\sum_{t=0}^{T-1} e_d\left(ha\left(t\right)\right)\right|\cdot\left|\sum_{x=0}^{H_s} e_d\left(-2hx\right)\right|. \end{aligned} \tag{22}$$

Note that given a divisor $d>1$ of M, $[h\underline{a}]_{\bmod d}$ is a primitive sequence over $\mathbf{Z}/(d)$ with period $\lambda\left(d\right)$ for every integer h coprime with d, and so it follows from Lemma 8 and Remark 9 that

$$\left|\sum_{t=0}^{T-1} e_d\left(ha\left(t\right)\right)\right| = \left|\frac{T}{\lambda\left(d\right)}\cdot\sum_{t=0}^{\lambda(d)-1} e_d\left(ha\left(t\right)\right)\right| \leq \frac{T\cdot d^{1/2}}{\lambda\left(d\right)}. \tag{23}$$

Combining (22) and (23) yields

$$\begin{aligned} & \left| N\left(\underline{v}^T, s\right) - \frac{T \cdot (H_s+1)}{M} \right| \\ \leq\ & \frac{1}{M} \sum_{\substack{d \mid M \\ d>1}} \sum_{\substack{1 \leq h \leq d-1 \\ \gcd(h,d)=1}} \frac{T \cdot d^{1/2}}{\lambda(d)} \cdot \left| \sum_{x=0}^{H_s} e_d(-2hx) \right| \\ =\ & \frac{T}{M} \sum_{\substack{d \mid M \\ d>1}} \frac{d^{1/2}}{\lambda(d)} \cdot \sum_{\substack{1 \leq h \leq d-1 \\ \gcd(h,d)=1}} \left| \sum_{x=0}^{H_s} e_d(-2hx) \right| \\ \leq\ & \frac{T}{M} \sum_{\substack{d \mid M \\ d>1}} \frac{d^{1/2}}{\lambda(d)} \cdot \sum_{h=1}^{d-1} \left| \sum_{x=0}^{H_s} e_d(-2hx) \right|. \end{aligned} \tag{24}$$

Since $\gcd(2, d) = 1$, we get

$$\sum_{h=1}^{d-1} \left| \sum_{x=0}^{H_s} e_d(-2hx) \right| = \sum_{h=1}^{d-1} \left| \sum_{x=0}^{H_s} e_d(hx) \right|. \tag{25}$$

Applying Lemma 6 to the right-hand side of (25) we obtain

$$\sum_{h=1}^{d-1} \left| \sum_{x=0}^{H_s} e_d(-2hx) \right| < 2d \cdot \left(\frac{\ln d}{\pi} + \frac{1}{5} \right), \tag{26}$$

and so the result follows from (24) and (26). ■

The following Theorem 15 immediately follows from Lemma 14.

Theorem 15 *Let* $\underline{a}$ *be a primitive sequence of order* 1 *over* $\mathbf{Z}/(M)$. *Then there exists an even number occurring in* $\underline{a}$ *if*

$$\frac{M+1}{4} \geq \sum_{\substack{d \mid M \\ d>1}} \frac{d^{3/2}}{\lambda(d)} \cdot \left(\frac{\ln d}{\pi} + \frac{1}{5} \right). \tag{27}$$

Experiments show that there are about 69.720%, 75.862%, 80.787%, 87.459% and 90.619% of M's satisfying (27) among all M's less than $100,000$, $300,000$, $1,000,000$, $10,000,000$ and $50,000,000$, respectively. It can be seen that the percentage increases as the range of M increases.

In fact, our experiments even indicate the following conjecture which has been verified for all M's less than $300,000$.

Conjecture 16 *For every primitive sequence $\underline{a}$ of order 1 over $\mathbf{Z}/(M)$, there exists an even number occurring in $\underline{a}$.*

Remark 17 *Conjecture 16 implies that for every primitive element $\xi \in \mathbf{Z}/(M)$, there exists an integer $t \geq 0$ such that $\left[\xi^t\right]_{\bmod M}$ is a positive even number.*

Remark 18 *If Conjecture 16 is true, then for every typical primitive polynomial $f(x)$ over $\mathbf{Z}/(M)$, there always exist a positive integer S and a positive even number $C < M$ such that $x^S \equiv C \bmod f(x)$ holds over $\mathbf{Z}/(M)$. This is because by Lemma 1, if $f(x)$ is a typical primitive polynomial over $\mathbf{Z}/(M)$, then $x^{S_0} \equiv \xi \bmod f(x)$ holds over $\mathbf{Z}/(M)$ for some positive integer S_0 and some primitive element ξ in $\mathbf{Z}/(M)$, and so it follows from Remark 17 that there exists an integer $t \geq 0$ such that $C = \left[\xi^t\right]_M$ is a positive even number. Thus we get $x^{S_0 t} \equiv \xi^t \equiv C \bmod f(x)$ holds over $\mathbf{Z}/(M)$.*

Although we could not completely prove Conjecture 16 by now, we obtain a asymptotic result as follows.

Let I be a set of positive integers and S a subset of I. For any positive integer n, denote

$$I_n = \{m \in I \mid m \leq n\} \text{ and } S_n = \{m \in S \mid m \leq n\}.$$

The asymptotic density of S is the following limit (if it exists)

$$\rho(S) = \lim_{n \to \infty} \frac{\#S_n}{\#I_n},$$

where $\#S_n$ and $\#I_n$ are the number of elements in S_n and I_n, respectively.

Theorem 19 *Let I be the set of all square-free odd integers. There is a subset S of I with asymptotic density 1 such that Conjecture 16 is true for $M \in S$.*

Proof. See Appendix B. ■

4 The distinctness of primitive sequences over $\mathbf{Z}/(M)$ modulo 2

This section is mainly devoted to the proof of Theorem 20.

Theorem 20 *Let $f(x)$ be a typical primitive polynomial of degree $n = 2k+1$ over $\mathbf{Z}/(M)$ with $k \geq 1$. If*

(1) Conjecture 16 is true; and

(2) for any sequence $\underline{z} \in G'(f(x), M)$, there exist two nonnegative integers t_1 and t_2 such that $z(t_1) = 0$ and $z(t_2) \in \{1, M-1\}$; and

(3) (M, n) is a distinguishable pair,
then for $\underline{a}, \underline{b} \in G'(f(x), M)$, $\underline{a} = \underline{b}$ if and only if $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$.

We first give some necessary lemmas.

Lemma 21 *Let $f(x)$ be a typical primitive polynomial of degree $n = 2k+1$ over $\mathbf{Z}/(M)$ with $k \geq 1$, and let $\underline{a}, \underline{b} \in G'(f(x), M)$ with $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$. If*

(1) Conjecture 16 is true; and

(2) for any sequence $\underline{z} \in G'(f(x), M)$, there exists a nonnegative integer t such that $z(t) \in \{1, M-1\}$,
then there is a divisor $R > 1$ of M such that

$$[\underline{a}]_{\bmod R} = [\underline{b}]_{\bmod R}$$

but

$$[\underline{a}]_{\bmod q} \neq [\underline{b}]_{\bmod q}$$

for any prime divisor q of M/R.

Proof. Set $\underline{c} = [\underline{a} - \underline{b}]_{\mathrm{mod}\, M}$. It is clear that $\underline{c} \in G(f(x), M)$. We claim that $\underline{c} \notin G'(f(x), M)$. Otherwise, by assumption there is an integer $t \geq 0$ such that $c\,(t) \in \{1, M-1\}$.

If $c\,(t) = 1$, i.e., $[a(t) - b(t)]_{\mathrm{mod}\, M} = 1$. Then $[a\,(t)]_{\mathrm{mod}\, 2} = [b\,(t)]_{\mathrm{mod}\, 2}$ implies that

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

Since $f\,(x)$ is a typical primitive polynomial over $\mathbf{Z}/(M)$, it follows from Remark 18 that there exist a positive integer S and a positive even number $C < M$ such that $x^S \equiv C \bmod f(x)$ holds over $\mathbf{Z}/(M)$, and so we get

$$a\,(t+S) = [C \cdot 0]_{\mathrm{mod}\, M} = 0 \ \text{ and } b\,(t+S) = [C \cdot (M-1)]_{\mathrm{mod}\, M} = M - C,$$

which yield

$$[a\,(t+S)]_{\mathrm{mod}\, 2} \neq [b\,(t+S)]_{\mathrm{mod}\, 2}\,,$$

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

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

Therefore, we get that $\underline{c} \notin G'(f(x), M)$. This implies that there at least exists a prime divisor p of M such that $\underline{a} \equiv \underline{b} \bmod p$. Let R be the largest divisor of M such that $\underline{a} = \underline{b} \bmod R$. Then R is the desired divisor. ■

Lemma 22 *Let $f(x)$ be a typical primitive polynomial of degree $n = 2k+1$ over $\mathbf{Z}/(M)$ with $k \geq 1$ and $\underline{a}, \underline{b} \in G'(f(x), M)$. Then $[\underline{a}]_{\mathrm{mod}\, 2} \neq [\underline{b}]_{\mathrm{mod}\, 2}$ if*

(1) *Conjecture 16 is true; and*

(2) *$a\,(t^*) = 0$ and $b\,(t^*) = M - R$ for some nonnegative integer t^* and some divisor R of M with $1 < R < M$.*

Proof. Since $f(x)$ is a typical primitive polynomial over $\mathbf{Z}/(M)$, there exist a positive integer S and a primitive element ξ of $\mathbf{Z}/(M)$ such that $x^S \equiv \xi \bmod f\,(x)$ holds over $\mathbf{Z}/(M)$. Applying $x^S \equiv \xi \bmod f\,(x)$ to $\underline{a}$ and $\underline{b}$, respectively, we get

$$a\,(t^* + k \cdot S) = \left[a\,(t^*) \cdot \xi^k\right]_{\mathrm{mod}\, M} = 0$$

and

$$b\left(t^{*}+k\cdot S\right)=\left[b\left(t^{*}\right)\cdot\xi^{k}\right]_{\operatorname{mod}M}=M-R\cdot\left[\xi^{k}\right]_{\operatorname{mod}M/R}$$

for any integer $k\geq 0$. By Remark 17 there is an integer $k^{*}\geq 0$ such that $\left[\xi^{k^{*}}\right]_{\operatorname{mod}M/R}$ is a positive even number. Note that $\left[\xi^{k^{*}}\right]_{\operatorname{mod}M/R}\neq 0$, and so we get

$$\left[a\left(t^{*}+k^{*}\cdot S\right)\right]_{\operatorname{mod}2}=0\neq 1=\left[b\left(t^{*}+k^{*}\cdot S\right)\right]_{\operatorname{mod}2}.$$

This implies that $[\underline{a}]_{\operatorname{mod}2}\neq[\underline{b}]_{\operatorname{mod}2}$. ■

Lemma 23 *Let a and b be two positive integers with $\gcd(a,b)=1$. Then for any two nonnegative integers t_1 and t_2, there exist two integers k_1 and k_2 such that $t_1+k_1\cdot a=t_2+k_2\cdot b$.*

Proof. Since $\gcd(a,b)=1$, by the extended Euclidean algorithm there exist two integers u and v satisfying $u\cdot a+v\cdot b=1$. Then we get $(t_2-t_1)\cdot u\cdot a+(t_2-t_1)\cdot v\cdot b=t_2-t_1$, i.e., $t_1+(t_2-t_1)\cdot u\cdot a=t_2+(t_1-t_2)\cdot v\cdot b$, and so the lemma follows by setting $k_1=(t_2-t_1)\cdot u$ and $k_2=(t_1-t_2)\cdot v$. ■

Lemma 24 *Let $f(x)$ be a primitive polynomial over $\mathbf{Z}/(M)$, and let $d>1$ be a divisor of M, and let s be a given element in $\mathbf{Z}/(M)$. If for any sequence $\underline{z}\in G'(f(x),M)$, the element s occurs in $\underline{z}$, then for any sequence $\underline{m}\in G'(f(x),d)$, the element $[s]_{\operatorname{mod}d}$ occurs in $\underline{m}$.*

Proof. Since $\underline{m}$ can be lifted to be a sequence $\underline{z}$ in $G'(f(x),M)$ such that $\underline{m}=[\underline{z}]_{\operatorname{mod}d}$, it is easy to see that the lemma holds. ■

With the above preparations, now we are ready to prove Theorem 20.

Proof of Theorem 20. Since the necessary condition is trivial, in the following, we only prove the sufficient condition.

If $\underline{a}, \underline{b} \in G'(f(x), M)$ and $[\underline{a}]_{\bmod 2} = [\underline{b}]_{\bmod 2}$, then Lemma 21 (Note that $f(x)$ here is a typical primitive polynomial over $\mathbf{Z}/(M)$ since (M, n) is a distinguishable pair) implies that there is a divisor $R > 1$ of M such that

$$[\underline{a}]_{\bmod R} = [\underline{b}]_{\bmod R}$$

but

$$[\underline{a}]_{\bmod q} \neq [\underline{b}]_{\bmod q}$$

for any prime divisor q of M/R. Hence it suffices to show that $R = M$.

Suppose $R < M$. Let us denote $Q = M/R$. Note that M is a square-free odd integer, and so R and Q are square-free odd integers and $\gcd(R, Q) = 1$. Since $[\underline{a}]_{\bmod R} = [\underline{b}]_{\bmod R}$, by the Chinese Remainder Theorem, $\underline{a}$ and $\underline{b}$ can be written as

$$\underline{a} = [Q \cdot \underline{m}_1 + R \cdot \underline{m}_2]_{\bmod M} \text{ and } \underline{b} = [Q \cdot \underline{m}_1 + R \cdot \underline{m}_3]_{\bmod M}\,, \tag{28}$$

where

$$\underline{m}_1 \in G'(f(x), R) \text{ and } \underline{m}_2, \underline{m}_3 \in G'(f(x), Q).$$

Since $[\underline{a}]_{\bmod q} \neq [\underline{b}]_{\bmod q}$ for any prime divisor q of Q and $\underline{a} - \underline{b} \equiv R \cdot (\underline{m}_2 - \underline{m}_3) \bmod M$, it follows that $[\underline{m}_2]_{\bmod q} \neq [\underline{m}_3]_{\bmod q}$ for any prime divisor q of Q, which implies that $[\underline{m}_2 - \underline{m}_3]_{\bmod Q} \in G'(f(x), Q)$.

Firstly, since $\underline{m}_1 \in G'(f(x), R)$ and $[\underline{m}_2 - \underline{m}_3]_{\bmod Q} \in G'(f(x), Q)$, it follows from the condition (2) of Theorem 20 and Lemma 24 that there exist two positive integers t_1 and t_2 such that

$$m_1(t_1) = 0 \tag{29}$$

and

$$[m_2(t_2) - m_3(t_2)]_{\bmod Q} = 1 \text{ or } Q - 1. \tag{30}$$

Secondly, suppose $R = r_1 r_2 \cdots r_u$ and $Q = q_1 q_2 \cdots q_v$ are the canonical factorizations of R and Q, respectively. Set

$$\theta_R = \operatorname{lcm}\left(\frac{r_1^n - 1}{r_1 - 1}, \ldots, \frac{r_u^n - 1}{r_u - 1}\right) \text{ and } T_Q = \operatorname{lcm}\left(q_1^n - 1, \ldots, q_v^n - 1\right).$$

Since (M, n) is a distinguishable pair, it follows that

$$\gcd\left(\frac{p_i^n - 1}{p_i - 1}, p_j^n - 1\right) = 1$$

for any pair of distinct prime divisors p_i and p_j of M. In particular, we have

$$\gcd\left(\frac{r_i^n - 1}{r_i - 1}, q_j^n - 1\right) = 1$$

for all $1 \leq i \leq u$ and all $1 \leq j \leq v$, and so we get $\gcd(\theta_R, T_Q) = 1$.

Thirdly, since $\gcd(\theta_R, T_Q) = 1$, by Lemma 23 there exist two integers k_1 and k_2 such that

$$t_1 + k_1 \cdot \theta_R = t_2 + k_2 \cdot T_Q.$$

Set

$$t^* = t_1 + k_1 \cdot \theta_R = t_2 + k_2 \cdot T_Q. \tag{31}$$

Note that $f(x)$ is also a typical primitive polynomial of degree n over $\mathbf{Z}/(R)$, and so by (2) of Lemma 1, there exists a primitive element ξ_R of $\mathbf{Z}/(R)$ such that $x^{\theta_R} \equiv \xi_R \bmod f(x)$ holds over $\mathbf{Z}/(R)$. Applying $x^{\theta_R} \equiv \xi_R \bmod f(x)$ to $\underline{m}_1$ we can get

$$m_1(t_1 + k_1 \cdot \theta_R) = \left[m_1(t_1) \cdot (\xi_R)^{k_1}\right]_{\operatorname{mod} R} = 0. \tag{32}$$

Since T_Q is the period of $\underline{m}_2$ and $\underline{m}_3$, we have

$$m_2(t_2 + k_2 \cdot T_Q) = m_2(t_2) \text{ and } m_3(t_2 + k_2 \cdot T_Q) = m_3(t_2). \tag{33}$$

Then (28), (31), (32) and (33) yield

$$\begin{aligned} a(t^*) &= [Q \cdot m_1(t^*) + R \cdot m_2(t^*)]_{\operatorname{mod} M} \\ &= [Q \cdot m_1(t_1 + k_1 \cdot \theta_R) + R \cdot m_2(t_2 + k_2 \cdot T_Q)]_{\operatorname{mod} M} \\ &= R \cdot m_2(t_2) \end{aligned} \tag{34}$$

and

$$\begin{aligned} b(t^*) &= [Q \cdot m_1(t^*) + R \cdot m_3(t^*)]_{\operatorname{mod} M} \\ &= [Q \cdot m_1(t_1 + k_1 \cdot \theta_R) + R \cdot m_3(t_2 + k_2 \cdot T_Q)]_{\operatorname{mod} M} \\ &= R \cdot m_3(t_2). \end{aligned} \tag{35}$$

Finally, if $[m_2(t_2) - m_3(t_2)]_{\bmod Q} = 1$, then we get

$$\begin{cases} 0 < m_2(t_2) = w < Q \\ m_3(t_2) = w - 1 \end{cases} \text{ or } \begin{cases} m_2(t_2) = 0 \\ m_3(t_2) = Q - 1 \end{cases}.$$

If

$$\begin{cases} 0 < m_2(t_2) = w < Q, \\ m_3(t_2) = w - 1, \end{cases}$$

then (34) and (35) together with the fact that R is an odd integer give

$$[a(t^*)]_{\bmod 2} = [R \cdot w]_{\bmod 2} = [w]_{\bmod 2} \neq [w-1]_{\bmod 2} = [R \cdot (w-1)]_{\bmod 2} = [b(t^*)]_{\bmod 2},$$

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

$$\begin{cases} m_2(t_2) = 0, \\ m_3(t_2) = Q - 1, \end{cases}$$

then (34) and (35) yield

$$a(t^*) = 0 \text{ and } b(t^*) = M - R.$$

By Lemma 22 we get $[\underline{a}]_{\bmod 2} \neq [\underline{b}]_{\bmod 2}$, a contradiction.

Similarly, we can show $[\underline{a}]_{\bmod 2} \neq [\underline{b}]_{\bmod 2}$ if $[m_2(t_2) - m_3(t_2)]_{\bmod Q} = Q - 1$.

Therefore, we have that $R = M$. This completes the proof. ■

The following Corollary 25 immediately follows from Theorem 11 and Theorem 20.

Corollary 25 *Let $f(x)$ be a typical primitive polynomial of degree $n = 2k+1$ over $\mathbf{Z}/(M)$ with $k \geq 1$. If*

(1) *Conjecture 16 is true; and*

(2) $\left(1 - \sum_{i=1}^{r} \frac{p_i - 1}{p_i^n - 1}\right) > \sum_{k=2}^{r} \sum_{1 \leq i_1 < \cdots < i_k \leq r} \frac{\prod_{j=1}^{k} \left(p_{i_j} - 1\right) p_{i_j}^{n/2}}{\mathrm{lcm}\left(p_{i_1}^n - 1, p_{i_2}^n - 1, \ldots, p_{i_k}^n - 1\right)}$*; and*

(3) *(M, n) is a distinguishable pair,*

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

Remark 26 *Experiment shows that there are about* 61.148% *of* (M, n)*'s satisfying conditions* (2) *and* (3) *of Corollary 25 when* M *runs through all possible values between* 1 *and* $10,000,000$ *and* n *runs through all odd integers between* 3 *and* 19*.*

Note that Conjecture 16 naturally holds for the case of prime numbers, and so we can immediately get the following Corollary 27 by replacing the condition (1) of Corollary 25 with the estimate of Theorem 15.

Corollary 27 *Let* $f(x)$ *be a typical primitive polynomial of degree* $n = 2k + 1$ *over* $\mathbf{Z}/(M)$ *with* $k \geq 1$*. If*

(1) $\frac{Q+1}{4} \geq \sum\limits_{\substack{d|Q \\ d>1}} \frac{d^{3/2}}{\lambda(d)} \cdot \left(\frac{\ln d}{\pi} + \frac{1}{5}\right)$ *for every nonprime divisor* Q *of* M*; and*

(2) $\left(1 - \sum_{i=1}^{r} \frac{p_i - 1}{p_i^n - 1}\right) > \sum_{k=2}^{r} \sum_{1 \leq i_1 < \cdots < i_k \leq r} \frac{\prod_{j=1}^{k} \left(p_{i_j} - 1\right) p_{i_j}^{n/2}}{\mathrm{lcm}\left(p_{i_1}^n - 1, p_{i_2}^n - 1, \ldots, p_{i_k}^n - 1\right)}$*; and*

(3) (M, n) *is a distinguishable pair,*

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

Remark 28 *Experiment shows that there are about* 38.403% *of* (M, n)*'s satisfying the conditions of Corollary 27 when* M *runs through all possible values between* 1 *and* $10,000,000$ *and* n *runs through all odd integers between* 3 *and* 19*.*

5 Conclusion

Let m be an integer greater than 1. This paper studies the distinctness problem of primitive sequences over $\mathbf{Z}/\left(m\right)$ modulo 2. For the case of $m = p^e$, a prime power, the problem was completely solved in [19]. For the case of $m = pq$, a product of two distinct prime numbers, [21] first gave a partial answers, and then [18] almost completely solved it with the help of convincing experimental data. Consequently, the aim of this paper is trying to tackle any square-free modulus and a class of primitive sequences of order $2k+1$ is proved to be distinct modulo 2. It is not surprising to find that as the number of prime factors of the modulus m increases, the problem becomes more and more resistant to be solved. Thus to improve the results of this paper and to completely solve this problem for general modulus will rely on more profound results in number theory.

Appendix A: Proof of Theorem 13

As a preparation, we first introduce a result of Bugeaud, Corvaja and Zannier [24].

Lemma 29 *([24, Theorem 1]) If $a < b$ are two integers greater than 1 which are multiplicatively independent (that is, 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*

$$\gcd\left(a^n - 1, b^n - 1\right) < a^{n\varepsilon} \textit{ for all integers } n > N_\varepsilon.$$

Proof of Theorem 13. Since the left-hand side of (21) is equal to 1 as $n \to \infty$, it suffices to show that the right-hand side of (21) is equal to 0 as $n \to \infty$, i.e.,

$$\lim_{n\to\infty} \sum_{k=2}^{r} \sum_{1\le i_1<\cdots<i_k\le r} \frac{\prod_{j=1}^{k}(p_{i_j}-1)p_{i_j}^{n/2}}{\operatorname{lcm}\left(p_{i_1}^n - 1, p_{i_2}^n - 1, \ldots, p_{i_k}^n - 1\right)} = 0. \tag{36}$$

Recall that $M = p_1 p_2 \cdots p_r$ is the canonical factorization of M with $3 \le p_1 < p_2 < \cdots < p_r$. Given a real number $\varepsilon > 0$. For any $1 \le i < j \le r$, it follows from Lemma 29 that there exists an integer $N_\varepsilon^{(i,j)}$ such that

$$\gcd\left(p_i^n - 1, p_j^n - 1\right) < p_i^{n\varepsilon} \text{ for all integers } n > N_\varepsilon^{(i,j)}.$$

Set

$$N_\varepsilon = \max\{\left\lceil \frac{\ln p_i}{\ln p_1} \cdot N_\varepsilon^{(i,j)} \right\rceil \mid 1 \le i < j \le r\},$$

where $\lceil a \rceil$ denotes the smallest integer greater than or equal to a. Then it is clear that

$$\gcd\left(p_i^n - 1, p_j^n - 1\right) < p_1^{n\varepsilon},\ 1 \le i < j \le r \text{ and } n > N_\varepsilon. \tag{37}$$

Let $2 \le k \le r$ and $1 \le i_1 < \cdots < i_k \le r$. It follows from (37) that if $n > N_\varepsilon$, then

$$\begin{aligned}\operatorname{lcm}\left(p_{i_1}^n - 1, p_{i_2}^n - 1, \ldots, p_{i_k}^n - 1\right) &\ge \frac{\prod_{j=1}^k (p_{i_j}^n - 1)}{\prod_{1\le j<s\le k} \gcd(p_{i_j}^n - 1, p_{i_s}^n - 1)} \\ &\ge p_1^{-k^2 n\varepsilon/2} \cdot \prod_{j=1}^k (p_{i_j}^n - 1) \\ &\ge p_1^{-r^2 n\varepsilon/2} \cdot \prod_{j=1}^k (p_{i_j}^n - 1).\end{aligned}$$

Consequently, we have

$$\begin{aligned}\frac{\prod_{j=1}^k (p_{i_j} - 1) p_{i_j}^{n/2}}{\operatorname{lcm}\left(p_{i_1}^n - 1, p_{i_2}^n - 1, \ldots, p_{i_k}^n - 1\right)} &\le p_1^{r^2 n\varepsilon/2} \cdot \prod_{j=1}^k \frac{\left(p_{i_j} - 1\right) p_{i_j}^{n/2}}{p_{i_j}^n - 1} \\ &< p_1^{r^2 n\varepsilon/2} \cdot \prod_{j=1}^k p_{i_j}^{1-n/2} \\ &\le p_1^{r^2 n\varepsilon/2} \cdot M \cdot \prod_{j=1}^k p_{i_j}^{-n/2}. \qquad (38)\end{aligned}$$

Note that $k \ge 2$ and $p_{i_j} > p_1$ for $1 \le j \le k$, and so (38) yields

$$\frac{\prod_{j=1}^k (p_{i_j} - 1) p_{i_j}^{n/2}}{\operatorname{lcm}\left(p_{i_1}^n - 1, p_{i_2}^n - 1, \ldots, p_{i_k}^n - 1\right)} < p_1^{r^2 n\varepsilon/2} \cdot M \cdot p_1^{-nk/2} \le p_1^{r^2 n\varepsilon/2} \cdot M \cdot p_1^{-n} = M \cdot p_1^{-\frac{n}{2}\cdot(2 - r^2\varepsilon)}.$$

Hence it can be seen that

$$\sum_{k=2}^r \sum_{1\le i_1<\cdots<i_k\le r} \frac{\prod_{j=1}^k (p_{i_j} - 1) p_{i_j}^{n/2}}{\operatorname{lcm}\left(p_{i_1}^n - 1, p_{i_2}^n - 1, \ldots, p_{i_k}^n - 1\right)} < 2^r \cdot M \cdot p_1^{-\frac{n}{2}\cdot\left(2 - r^2\varepsilon\right)}.$$

Then choosing $\varepsilon < r^{-2}$, we get

$$0 \le \sum_{k=2}^r \sum_{1\le i_1<\cdots<i_k\le r} \frac{\prod_{j=1}^k (p_{i_j} - 1) p_{i_j}^{n/2}}{\operatorname{lcm}\left(p_{i_1}^n - 1, p_{i_2}^n - 1, \ldots, p_{i_k}^n - 1\right)} < 2^r \cdot M \cdot p_1^{-n/2}. \qquad (39)$$

Since r, M and p_1 are all fixed integers with $p_1 \ge 3$, then $2^r \cdot M \cdot p_1^{-n/2}$ is equal to 0 as $n \to \infty$, and so (36) follows from (39). ■

Appendix B: Proof of Theorem 19

Lemma 30 *([26, Theorem 2]) Let $\mathbb{N}^+$ be the set of all positive integers. There is a subset S of $\mathbb{N}^+$ with asymptotic density* 1 *such that, for $m \in S$,*

$$\lambda(m) = m/\left(\ln m\right)^{\ln\ln\ln m + A + O((\ln\ln\ln m)^{-1+\varepsilon})},$$

where $A = 0.2269688\ldots$ *and* $\varepsilon > 0$ *is fixed but arbitrarily small.*

Let I be the set of all square-free odd integers. Note that the asymptotic density of I in $\mathbb{N}^+$ is $\frac{4}{\pi^2} \neq 0$ (see [27, Theorem 1]), and so by Lemma 30 we can easily get the following Corollary 31.

Corollary 31 *Let I be the set of all square-free odd integers. There is a subset S of I with asymptotic density* 1 *such that, for* $m \in S$,

$$\lambda(m) = m / (\ln m)^{\ln\ln\ln m + A + O((\ln\ln\ln m)^{-1+\varepsilon})},$$

where $A = 0.2269688\ldots$ *and* $\varepsilon > 0$ *is fixed but arbitrarily small.*

As usual, for an integer $m \geq 1$ we denote by $\tau(m)$ the number of distinct positive integer divisors of m. We will make use of the following estimate of $\tau(m)$:

$$\ln \tau(m) = O\left(\frac{\ln m}{\ln\ln(m+2)}\right), \tag{40}$$

see [28, Theorem 5.2].

With the above preparations, we now can prove Theorem 19.

Proof of Theorem 19. By Theorem 15, it suffices to prove that there is a subset S of I with asymptotic density 1 such that the inequality

$$\frac{m+1}{4} \geq \sum_{\substack{d \mid m \\ d>1}} \frac{d^{3/2}}{\lambda(d)} \cdot \left(\frac{\ln d}{\pi} + \frac{1}{5}\right) \tag{41}$$

holds for $m \in S$.

Let m be a square-free odd integer and $d > 1$ a divisor of m. Note that

$$\lambda(m) = \operatorname{lcm}(\lambda(m/d), \lambda(d)) \leq \lambda(m/d) \cdot \lambda(d),$$

and

$$\lambda(m/d) < m/d \leq (m/d)^{3/2},$$

and so

$$\frac{d^{3/2}}{\lambda\left(d\right)} \leq \frac{m^{3/2}}{\lambda\left(m\right)}. \tag{42}$$

Applying (42) to the right-hand side of (41) we get

$$\begin{aligned}\sum_{\substack{d|m\\d>1}} \frac{d^{3/2}}{\lambda\left(d\right)} \cdot \left(\frac{\ln d}{\pi} + \frac{1}{5}\right) &\leq \sum_{\substack{d|m\\d>1}} \frac{m^{3/2}}{\lambda\left(m\right)} \cdot \left(\frac{\ln m}{\pi} + \frac{1}{5}\right)\\ &< \tau\left(m\right) \cdot \frac{m^{3/2}}{\lambda\left(m\right)} \cdot \left(\frac{\ln m}{\pi} + \frac{1}{5}\right)\\ &< C \cdot \tau\left(m\right) \cdot \frac{m^{3/2}}{\lambda\left(m\right)} \cdot \ln m,\end{aligned}$$

where C is some absolute constant. Hence the inequality (41) holds if

$$\frac{m}{4} \geq C \cdot \tau\left(m\right) \cdot \frac{m^{3/2}}{\lambda\left(m\right)} \cdot \ln m. \tag{43}$$

It follows from Corollary 31 that there is a subset $S^{'}$ of I with asymptotic density 1 such that for $m \in S^{'}$,

$$\lambda(m) = m/\left(\ln m\right)^{\ln\ln\ln m + A + O\left((\ln\ln\ln m)^{-1+\varepsilon}\right)}, \tag{44}$$

where $A = 0.2269688\ldots$ and $\varepsilon > 0$ is fixed but arbitrarily small. Note that $\tau\left(m\right) = O\left(m^{1/\ln\ln(m+2)}\right)$, and so the right-hand side of (43) is

$$O\left(m^{\frac{1}{2}+\frac{1}{\ln\ln(m+2)}}\left(\ln m\right)^{\ln\ln\ln m + 1 + A + O\left((\ln\ln\ln m)^{-1+\varepsilon}\right)}\right). \tag{45}$$

It can be seen that (45) is $m^{1/2+o(1)}$ as $m \to \infty$. Therefore there exists an integer N such that the inequality (43) holds for $m \in S^{'}$ and $m \geq N$. Set

$$S = \{m \in S^{'} \mid m \geq N\}.$$

Then S is also a subset of I with asymptotic density 1 and the inequality (41) holds for $m \in S$. This completes the proof. ■

References

[1] M. Ward, “The arithmetical theory of linear recurring series,” *Trans. Amer. Math. Soc.,* vol. 35, pp. 600-628, 1933.

[2] M. Q. Huang, “Analysis and cryptologic evaluation of primitive sequences over an integer residue ring,” Ph.D. 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.,* vol. 30, pp. 139-143, 1992.

[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*, Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 1991, vol. 473, pp. 189-195.

[5] Z. D. Dai, “Binary sequences derived from ML-sequences over rings I: periods and minimal polynomials,” *J. Crypt.*, vol. 5, pp. 193-207, 1992.

[6] A. S. Kuzmin and A. A. Nechaev, “Linear recurring sequences over Galois ring,” *Russian Math. Surv.*, vol. 48, pp. 171-172, 1993.

[7] A. S. Kuzmin, G. B. Marshalko and A. A. Nechaev, “Reconstruction of a linear recurrence over a primary residue ring,” *Memoires in Discr. Math.*, vol. 12, pp. 155-194, 2009. (in Russian)

[8] D. N. Bylkov and A. A. Nechaev, “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.*, vol. 20, no. 5-6, pp. 591-609, 2010.

[9] A. S. Kuzmin, “Lower estimates for the ranks of coordinate sequences of linear recurrent sequences over primary residue rings of integers,” *Russian Math. Surv.*, vol. 48, pp. 203-204, 1993.

[10] W. F. Qi, J. H. Yang and J. J. Zhou, “ML-sequences over rings $\mathbf{Z}/(2^e)$,” in *Advances in Cryptology — ASIACRYPT’98*, Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 1998, vol. 1514, pp. 315-325.

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

[12] X. Y. Zhu and W. F. Qi, "Compression mappings on primitive sequences over $\mathbf{Z}/(p^e)$," *IEEE Trans. Inf. Theory*, vol. 50, pp. 2442-2448, 2004.

[13] X. Y. Zhu and W. F. Qi, "Further result of compressing maps on primitive sequences modulo odd prime powers," *IEEE Trans. Inf. Theory*, vol. 53, pp. 2985-2990, 2007.

[14] 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.*, vol. 11, pp. 30-44, 2005.

[15] 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.*, vol. 13, pp. 230-248, 2007.

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

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

[18] Q. X. Zheng and W. F. Qi, "A new result on the distinctness of primitive sequences over $\mathbf{Z}/(pq)$ modulo 2," *Finite Fields Appl.*, vol. 17, pp. 254-274, 2011.

[19] X. Y. Zhu and W. F. Qi, "On the distinctness of modular reductions of maximal length sequences modulo odd prime powers," *Math. Comp.*, vol. 77, pp. 1623-1637, 2008.

[20] A. Klapper and M. Goresky, "2-Adic shift registers," in *Fast Software Encryption,* Lecture Notes in Computer Science. Berlin, Germany: Springer-Verlag, 1993, vol. 809, pp. 174-178.

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

[22] T. Tian and W. F. Qi, “Typical primitive polynomials over integer residue rings,” *Finite Fields Appl.*, vol. 15, pp. 796-807, 2009.

[23] R. Lidl and H. Niederreiter, Finite Fields. Cambridge, U.K.: Cambridge Univ. Press, 1983.

[24] Y. Bugeaud, P. Corvaja and U. Zannier, “An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$,” Math. Z., vol. 243, pp. 79-84, 2003.

[25] R. D. Carmichael, “On composite numbers p which satisfy the Fermat congruence $a^{p-1} \equiv 1 \bmod p$,” *Amer. Math. Monthly*, vol. 19, pp. 22-27, 1912.

[26] P. Erdős, C. Pomerance and E. Schmutz, “Carmichael’s lambda function,” *Acta Arith.*, vol. 58, pp. 363-385, 1991.

[27] G. J. O. Jameson, “Even and odd square-free numbers,” Math. Gazette, vol. 94, pp. 123–127, 2010.

[28] K. Prachar, Primzahlverteilung. Springer-Verlag, Berlin, 1957.