AIMS Mathematics, 7(6): 11087–11101.
DOI:10.3934/math.2022619
Received: 25 November 2021
Revised: 22 March 2022
Accepted: 22 March 2022
Published: 07 April 2022

http://www.aimspress.com/journal/Math

Research article

Correlation measures of binary sequences derived from Euler quotients

Huaning Liu[1], **Zhixiong Chen**[2] **and Chenhuang Wu**[3,*]

[1] Research Center for Number Theory and Its Applications, School of Mathematics, Northwest University, Xi'an 710127, Shaanxi, China
[2] Fujian Key Laboratory of Financial Information Processing, Putian University, Putian 351100, Fujian, China
[3] Key Laboratory of Applied Mathematics of Fujian Province University, Putian University, Putian 351100, Fujian, China

* **Correspondence:** Email: ptuwch@163.com.

Abstract: Fermat-Euler quotients arose from the study of the first case of Fermat's Last Theorem, and have numerous applications in number theory. Recently they were studied from the cryptographic aspects by constructing many pseudorandom binary sequences, whose linear complexities and trace representations were calculated. In this work, we further study their correlation measures by introducing a new approach based on Dirichlet characters, Ramanujan sums and Gauss sums. Our results show that the 4-order correlation measures of these sequences are very large. Therefore they may not be suggested for cryptography.

Keywords: Euler quotient; binary sequence; correlation measure; character sum
Mathematics Subject Classification: 11B50, 11K45, 94A55, 94A60

1. Introduction

Let $\mathcal{S} = (s_0, s_1, ..., s_{T-1})$ be a binary sequence over $\mathbb{F}_2 = \{0, 1\}$ and ℓ a positive integer. Mauduit and Sárközy [16] introduced the correlation measure of order ℓ for $\mathcal{S}$, which is defined as

$$C_\ell(\mathcal{S}) = \max_{U,D} \left| \sum_{n=0}^{U-1} (-1)^{s_{n+d_1}+s_{n+d_2}+\ldots+s_{n+d_\ell}} \right|,$$

where the maximum is taken over all $U \in \mathbb{N}$ and $D = (d_1, d_2, \ldots, d_\ell)$ with integers $0 \le d_1 < d_2 < \ldots < d_\ell \le T - U$.

From the viewpoint of cryptography, it is excepted that measure of order ℓ of sequences is as "small" (in terms of T, in particular, is $o(T)$ as $T \to \infty$) as possible. Cassaigne, Mauduit and Sárközy [4]

studied the values of $C_\ell(\mathcal{S})$ for $\mathcal{S} \in \{0,1\}^T$ chosen equiprobable. It was shown in [4] that for every integer $\ell \geq 2$ and real $\varepsilon > 0$, there are numbers $T_0 = T_0(\varepsilon, \ell)$ and $\delta = \delta(\varepsilon, \ell) > 0$ such that for all $T \geq T_0$ we have

$$\delta \sqrt{T} < C_\ell(\mathcal{S}) < 5\sqrt{\ell T \log T}$$

with probability at least $1 - \varepsilon$.

Additionally, we use the following definition for the *periodic correlation measure of order* ℓ of $\mathcal{S}$,

$$\theta_\ell(\mathcal{S}) = \max_D \left| \sum_{n=0}^{T-1} (-1)^{s_{n+d_1} + s_{n+d_2} + \ldots + s_{n+d_\ell}} \right|,$$

where $D = (d_1, d_2, \ldots, d_\ell)$ and $0 \leq d_1 < d_2 < \ldots < d_\ell < T$. It is clear that $\theta_2(\mathcal{S})$ is the (classic) auto-correlation of $\mathcal{S}$ and $\theta_\ell(\mathcal{S}) \leq C_\ell(\mathcal{S})$. Thus for every integer $\ell \geq 2$ and real $\varepsilon > 0$, there is number $T_0 = T_0(\varepsilon, \ell)$ such that for all $T \geq T_0$ we have $\theta_\ell(\mathcal{S}) < 5\sqrt{\ell T \log T}$ with probability at least $1 - \varepsilon$.

In this work, we mainly consider the periodic correlation measure of order 4 for some binary sequences derived from Euler quotients studied recently.

Let p be a prime and let n be an integer with $\gcd(n, p) = 1$. From Fermat's little theorem we know that $n^{p-1} \equiv 1 \pmod{p}$. Then the Fermat quotient $Q_p(n)$ is defined as

$$Q_p(n) = \frac{n^{p-1} - 1}{p} \pmod{p}, \quad 0 \leq Q_p(n) < p.$$

We also define $Q_p(n) = 0$ if $\gcd(n, p) > 1$. Fermat quotients arose from the study of the first case of Fermat's last theorem, and have many applications in number theory (see [2,5,12,14,17,19–21] for details). Define the p^2-periodic binary sequence $\overline{\mathbf{s}} = \left(\overline{s}_0, \overline{s}_1, \cdots, \overline{s}_{p^2-1}\right)$ by

$$\overline{s}_t = \begin{cases} 0, & \text{if } 0 \leq \frac{Q_p(t)}{p} < \frac{1}{2}, \\ 1, & \text{if } \frac{1}{2} \leq \frac{Q_p(t)}{p} < 1. \end{cases}$$

The second author (partially with other co-authors) studied the well-distribution measure and correlation measure of order 2 of $\overline{\mathbf{s}}$ by using estimates for exponential sums of Fermat quotients in [11], the linear complexity of $\overline{\mathbf{s}}$ in [7, 10], and the trace representation of $\overline{\mathbf{s}}$ by determining the defining pairs of all binary characteristic sequences of cosets in [6]. In [15] the first author with another co-author showed that the 4-order correlation measure of $\overline{\mathbf{s}}$ is very large.

Let $m \geq 2$ be an odd number and let n be an integer coprime to m. The Euler's theorem says that $n^{\phi(m)} \equiv 1 \pmod{m}$, where ϕ is the Euler's totient function. Then the Euler quotient $Q_m(n)$ is defined as

$$Q_m(n) = \frac{n^{\phi(m)} - 1}{m} \pmod{m}, \quad 0 \leq Q_m(n) < m.$$

We also define $Q_m(n) = 0$ if $\gcd(n, m) > 1$. Agoh, Dilcher and Skula [1] studied the detailed properties of Euler quotients. For example, from Proposition 2.1 of [1] we have

$$Q_m(n_1 n_2) \equiv Q_m(n_1) + Q_m(n_2) \pmod{m} \quad \text{for } n_1, n_2 \in \mathbb{Z} \text{ with } \gcd(n_1 n_2, m) = 1, \tag{1.1}$$

$$Q_m(n + cm) \equiv Q_m(n) + cn^{-1}\phi(m) \pmod{m} \quad \text{for } n, c \in \mathbb{Z} \text{ with } \gcd(n, m) = 1. \tag{1.2}$$

Recently many binary sequences were constructed from Euler quotients. For example, let $m = p^\tau$ for a fixed number $\tau \geq 1$, the $p^{\tau+1}$-periodic sequence $\widetilde{\mathbf{s}} = \left(\widetilde{s}_0, \widetilde{s}_1, \cdots, \widetilde{s}_{p^{\tau+1}-1}\right)$ is defined by

$$\widetilde{s}_t = \begin{cases} 0, & \text{if } 0 \leq \frac{Q_{p^\tau}(t)}{p^\tau} < \frac{1}{2}, \\ 1, & \text{if } \frac{1}{2} \leq \frac{Q_{p^\tau}(t)}{p^\tau} < 1. \end{cases} \tag{1.3}$$

The linear complexity of $\widetilde{\mathbf{s}}$ had been investigated in [13] and the trace representation of $\widetilde{\mathbf{s}}$ was given in [8].

Moreover, let $m = pq$ be an odd semiprime with $p \mid (q-1)$, the pq^2-periodic sequence $\widehat{\mathbf{s}} = \left(\widehat{s}_0, \widehat{s}_1, \cdots, \widehat{s}_{pq^2-1}\right)$ is defined by

$$\widehat{s}_t = \begin{cases} 0, & \text{if } 0 \leq \frac{Q_{pq}(t)}{pq} < \frac{1}{2}, \\ 1, & \text{if } \frac{1}{2} \leq \frac{Q_{pq}(t)}{pq} < 1. \end{cases} \tag{1.4}$$

Recently the minimal polynomials and linear complexities were determined in [22] for $\widehat{\mathbf{s}}$, and the trace representation of $\widehat{\mathbf{s}}$ has been given in [23] provided that $2^{q-1} \not\equiv 1 \pmod{q^2}$.

In this work, we shall further study the (periodic) correlation measures of $\widetilde{\mathbf{s}}$ and $\widehat{\mathbf{s}}$ by introducing a new approach based on Dirichlet characters, Ramanujan sums and Gauss sums. We state below the main result.

Theorem 1.1. *Let $k \geq 5$ be a prime and let m be an odd number with $k \mid m$. Suppose that $Q_m(n)$ is km-periodic and the km-periodic sequence $\mathbf{s} = (s_0, s_1, \cdots, s_{km-1}) \in \{0,1\}^{km}$ is defined by*

$$s_t = \begin{cases} 0, & \text{if } 0 \leq \frac{Q_m(t)}{m} < \frac{1}{2}, \\ 1, & \text{if } \frac{1}{2} \leq \frac{Q_m(t)}{m} < 1. \end{cases} \tag{1.5}$$

Then there exists absolute constant $\delta > 0$ such that

$$\sum_{t=0}^{km-1} (-1)^{s_t + s_{t+m} + s_{t+2m} + s_{t+3m}} \geq \frac{1}{3}km - \delta k^{\frac{1}{2}} m (\log m)^4.$$

The restriction $k \geq 5$ can not be relaxed since otherwise we have $s_t = s_{t+3m}$ for all $0 \leq t \leq km-1$. The assumptions $k \mid m$, k is a prime and m is odd will be vital in the proof of Lemmas 2.1 and 2.2 in Section 2. Taking special values of m and k in Theorem 1.1, we immediately get the correlation measures of $\widetilde{\mathbf{s}}$ and $\widehat{\mathbf{s}}$.

Corollary 1.1. *Let $p \geq 5$ be a prime and let $\tau \geq 1$ be a fixed integer. Let the $p^{\tau+1}$-periodic sequence $\widetilde{\mathbf{s}} = \left(\widetilde{s}_0, \widetilde{s}_1, \cdots, \widetilde{s}_{p^{\tau+1}-1}\right)$ be defined as in* (1.3)*. Then we have*

$$\sum_{t=0}^{p^{\tau+1}-1} (-1)^{\widetilde{s}_t + \widetilde{s}_{t+p^\tau} + \widetilde{s}_{t+2p^\tau} + \widetilde{s}_{t+3p^\tau}} \geq \frac{1}{3}p^{\tau+1} - \delta p^{\tau+\frac{1}{2}} (\log p^\tau)^4.$$

Corollary 1.2. *Let p and q be two distinct odd primes with $p \mid (q-1)$ and $q \geq 5$, and let the pq^2-periodic sequence $\widehat{\mathbf{s}} = \left(\widehat{s}_0, \widehat{s}_1, \cdots, \widehat{s}_{pq^2-1}\right)$ be defined as in* (1.4)*. Then we have*

$$\sum_{t=0}^{pq^2-1} (-1)^{\widehat{s}_t + \widehat{s}_{t+pq} + \widehat{s}_{t+2pq} + \widehat{s}_{t+3pq}} \geq \frac{1}{3}pq^2 - \delta pq^{\frac{3}{2}} (\log pq)^4.$$

Our results indicate that the correlation measures of order 4 of $\widetilde{\mathbf{s}}$ and $\widehat{\mathbf{s}}$ are very large provided that p and q are sufficiently large. Therefore these sequences are not suitable for cryptography.

To prove Theorem 1.1, we introduce basic properties of Dirichlet characters, Ramanujan sums and Gauss sums, and then prove two lemmas on the mean values of characters sums in Section 2. We express $(-1)^{s_t}$ in terms of character sums in Section 3 to finish the proof of Theorem 1.1 by using the results showed in Section 2.

We write $f(n) = O(g(n))$ or $f(n) \ll g(n)$ if $|f(n)| \le cg(n)$ for some absolute constant $c > 0$.

2. Dirichlet characters and Gauss sums

Let $N > 1$ be an integer. The Ramanujan sum is denoted by

$$c_N(n) = \sum_{\substack{t=0 \\ \gcd(t,N)=1}}^{N-1} e_N(tn),$$

where $e_N(x) = \mathrm{e}^{2\pi\sqrt{-1}x/N}$. We have

$$c_N(n) = \mu\left(\frac{N}{\gcd(n,N)}\right)\phi(N)\phi\left(\frac{N}{\gcd(n,N)}\right)^{-1}, \tag{2.1}$$

where μ is the Möbius function.

We recall that a Dirichlet character χ modulo N is a function satisfying:
(i). $\chi(t_1t_2) = \chi(t_1)\chi(t_2)$,
(ii). $\chi(t+N) = \chi(t)$,
(iii). $\chi(t) = 0$ for $\gcd(t,N) > 1$,
(iv). χ is not identically zero.

When $\chi(n) = 1$ for all n with $\gcd(n,N) = 1$ we say χ is the trivial character modulo N. An integer $d \mid N$ is called an induced modulus for χ if $\chi(a) = 1$ whenever $\gcd(a,N) = 1$ and $a \equiv 1 \pmod{d}$. A Dirichlet character χ mod N is said to be primitive mod N if it has no induced modulus $d < N$. The smallest induced modulus d for χ is called the conductor of χ. Every non-trivial character χ modulo N can be uniquely written as $\chi = \chi_0\chi^*$, where χ_0 is the trivial character modulo N and χ^* is the primitive character modulo the conductor of χ.

For a Dirichlet character χ mod N, the Gauss sum associated with χ is defined by

$$G(n,\chi) = \sum_{t=0}^{N-1}\chi(t)e_N(tn).$$

Let N^* be the conductor for χ and let χ^* be the induced primitive character.

Let N_1 be the maximal divisor of N such that N_1 and N^* have the same prime divisors. Then we have

$$G(n,\chi) = \begin{cases} \chi^*\left(\frac{n}{\gcd(n,N)}\right)^{-1}\chi^*\left(\frac{N}{N^*\gcd(n,N)}\right)\mu\left(\frac{N}{N^*\gcd(n,N)}\right) \\ \quad \times\phi(N)\phi\left(\frac{N}{\gcd(n,N)}\right)^{-1}G(1,\chi^*), & \text{if } N^* = \frac{N_1}{\gcd(n,N_1)}, \\ 0, & \text{if } N^* \ne \frac{N_1}{\gcd(n,N_1)}. \end{cases} \tag{2.2}$$

See Chapter 8 of [3] or Chapter 1 of [18] for more details of Dirichlet characters, Ramanujan sums and Gauss sums.

Now we prove two lemmas on the mean values of characters sums.

Lemma 2.1. *Let $k \geq 5$ be a prime and let m be an odd number with $k \mid m$. Let χ be a Dirichlet character modulo km such that χ^m is trivial and $\chi^{m'}$ is not trivial for all $1 \leq m' < m$. For integers a_1, a_2, a_3 and a_4 we have*

$$\sum_{t=0}^{km-1} \chi\left(t^{a_1}(t+m)^{a_2}(t+2m)^{a_3}(t+3m)^{a_4}\right) = \begin{cases} k\phi(m), & \text{if } m \mid (a_1+a_2+a_3+a_4) \text{ and } k \mid (a_2+2a_3+3a_4), \\ O\left(\phi(m)\phi(k)^{-1}k^{\frac{3}{2}}\right), & \text{otherwise.} \end{cases}$$

Proof. Note that if $k \geq 5$, then the polynomials t, $t+m$, $t+2m$ and $t+3m$ are distinct. By the condition $k \mid m$ and the properties of residue systems we get

$$\begin{aligned}
&\sum_{t=0}^{km-1} \chi\left(t^{a_1}(t+m)^{a_2}(t+2m)^{a_3}(t+3m)^{a_4}\right) \\
&= \sum_{\substack{y=0 \\ \gcd(y,m)=1}}^{m-1} \sum_{z=0}^{k-1} \chi\left((y+zm)^{a_1}(y+zm+m)^{a_2}(y+zm+2m)^{a_3}(y+zm+3m)^{a_4}\right) \\
&= \sum_{\substack{y=0 \\ \gcd(y,m)=1}}^{m-1} \sum_{z=0}^{k-1} \chi\left((y^{a_1}+a_1y^{a_1-1}zm)(y^{a_2}+a_2y^{a_2-1}(z+1)m)\right) \\
&\quad \times \chi\left((y^{a_3}+a_3y^{a_3-1}(z+2)m)(y^{a_4}+a_4y^{a_4-1}(z+3)m)\right) \\
&= \sum_{\substack{y=0 \\ \gcd(y,m)=1}}^{m-1} \chi\left(y^{a_1+a_2+a_3+a_4}\right) \\
&\quad \times \sum_{z=0}^{k-1} \chi\left((1+a_1y^{-1}zm)(1+a_2y^{-1}(z+1)m)(1+a_3y^{-1}(z+2)m)(1+a_4y^{-1}(z+3)m)\right).
\end{aligned}$$

By the condition $k \mid m$ we further deduce that

$$\begin{aligned}
&\chi(1+(n+k)m) = \chi(1+nm), \\
&\chi(1+n_1m)\chi(1+n_2m) = \chi(1+(n_1+n_2)m),
\end{aligned}$$

which show that $\chi(1+nm)$ is a non-trivial additive character modulo k. Since k is a prime, there is uniquely an integer β such that $1 \leq \beta \leq k-1$ and $\chi(1+nm) = e_k(\beta n)$. Hence,

$$\sum_{t=0}^{km-1} \chi\left(t^{a_1}(t+m)^{a_2}(t+2m)^{a_3}(t+3m)^{a_4}\right) = \sum_{\substack{y=0 \\ \gcd(y,m)=1}}^{m-1} \chi\left(y^{a_1+a_2+a_3+a_4}\right)$$

$$\times \sum_{z=0}^{k-1} e_k\left(\beta(a_1y^{-1}z + a_2y^{-1}(z+1) + a_3y^{-1}(z+2) + a_4y^{-1}(z+3))\right).$$

By the orthogonality relation for additive character

$$\sum_{u=0}^{N-1} e_N(u\theta) = \begin{cases} N, & \text{if } N \mid \theta, \\ 0, & \text{if } N \nmid \theta, \end{cases} \tag{2.3}$$

we have

$$\begin{aligned}
&\sum_{z=0}^{k-1} e_k\left(\beta(a_1y^{-1}z + a_2y^{-1}(z+1) + a_3y^{-1}(z+2) + a_4y^{-1}(z+3))\right) \\
&= e_k\left(\beta(a_2 + 2a_3 + 3a_4)y^{-1}\right) \sum_{z=0}^{k-1} e_k\left(\beta y^{-1}(a_1 + a_2 + a_3 + a_4)z\right) \\
&= \begin{cases} ke_k\left(\beta(a_2 + 2a_3 + 3a_4)y^{-1}\right), & \text{if } k \mid (a_1 + a_2 + a_3 + a_4), \\ 0, & \text{if } k \nmid (a_1 + a_2 + a_3 + a_4). \end{cases}
\end{aligned}$$

Then from

$$\begin{aligned}
&\sum_{t=0}^{km-1} \chi\left(t^{a_1}(t+m)^{a_2}(t+2m)^{a_3}(t+3m)^{a_4}\right) \\
&= \begin{cases} k \sum\limits_{\substack{y=0 \\ \gcd(y,m)=1}}^{m-1} \chi^{a_1+a_2+a_3+a_4}(y)\, e_k\left(\beta(a_2 + 2a_3 + 3a_4)y^{-1}\right), & \text{if } k \mid (a_1 + a_2 + a_3 + a_4), \\ 0, & \text{if } k \nmid (a_1 + a_2 + a_3 + a_4). \end{cases}
\end{aligned}$$

Since $k \mid m$, we know that $\chi^{a_1+a_2+a_3+a_4}$ is a multiplicative character modulo m if $k \mid a_1 + a_2 + a_3 + a_4$. Then

$$\sum_{\substack{y=0 \\ \gcd(y,m)=1}}^{m-1} \chi^{a_1+a_2+a_3+a_4}(y)\, e_k\left(\beta(a_2 + 2a_3 + 3a_4)y^{-1}\right) = \sum_{\substack{y=0 \\ \gcd(y,m)=1}}^{m-1} \chi^{-(a_1+a_2+a_3+a_4)}(y)\, e_m\left(\frac{m}{k}\beta(a_2 + 2a_3 + 3a_4)y\right)$$

is a Gauss sum associated with $\chi^{-(a_1+a_2+a_3+a_4)}$ modulo m. By the assumption χ^m is trivial and $\chi^{m'}$ is not trivial for all $1 \le m' < m$ we know that $\chi^{-(a_1+a_2+a_3+a_4)}$ is trivial if and only if $m \mid a_1 + a_2 + a_3 + a_4$. Then from (2.1) and (2.2) we get

$$\sum_{\substack{y=0 \\ \gcd(y,m)=1}}^{m-1} \chi^{-(a_1+a_2+a_3+a_4)}(y)\, e_m\left(\frac{m}{k}\beta(a_2 + 2a_3 + 3a_4)y\right) = \phi(m),$$

if $m \mid (a_1 + a_2 + a_3 + a_4)$ and $k \mid (a_2 + 2a_3 + 3a_4)$, and

$$\left| \sum_{\substack{y=0 \\ \gcd(y,m)=1}}^{m-1} \chi^{-(a_1+a_2+a_3+a_4)}(y)\, e_m\left(\frac{m}{k}\beta(a_2 + 2a_3 + 3a_4)y\right) \right|$$

$$\leq \begin{cases} \phi(m)\phi(k)^{-1}, & \text{if } m \mid (a_1+a_2+a_3+a_4) \text{ and } k \nmid (a_2+2a_3+3a_4), \\ 0, & \text{if } m \nmid (a_1+a_2+a_3+a_4) \text{ and } k \mid (a_2+2a_3+3a_4), \\ \phi(m)\phi(k)^{-1}k^{\frac{1}{2}}, & \text{if } m \nmid (a_1+a_2+a_3+a_4) \text{ and } k \nmid (a_2+2a_3+3a_4). \end{cases}$$

Therefore

$$\sum_{t=0}^{km-1} \chi\left(t^{a_1}(t+m)^{a_2}(t+2m)^{a_3}(t+3m)^{a_4}\right)$$
$$= \begin{cases} k\phi(m), & \text{if } m \mid (a_1+a_2+a_3+a_4) \text{ and } k \mid (a_2+2a_3+3a_4), \\ O\left(\phi(m)\phi(k)^{-1}k^{\frac{3}{2}}\right), & \text{otherwise.} \end{cases}$$

□

Lemma 2.2. *Let m be an odd number and let k be a positive integer with $k \leq m$. Define*

$$\Xi_{m,k} := \sum_{\substack{1\leq|a_1|,|a_2|,|a_3|,|a_4|\leq\frac{m-1}{2} \\ a_1+a_2+a_3+a_4\equiv 0 \pmod m \\ a_2+2a_3+3a_4\equiv 0 \pmod k}} \sum_{l_1=\frac{m+1}{2}}^{m-1} e_m(-a_1l_1) \sum_{l_2=\frac{m+1}{2}}^{m-1} e_m(-a_2l_2)$$
$$\times \sum_{l_3=\frac{m+1}{2}}^{m-1} e_m(-a_3l_3) \sum_{l_4=\frac{m+1}{2}}^{m-1} e_m(-a_4l_4).$$

Then we have

$$\Xi_{m,k} = \frac{1}{48}m^4 + O\left(\frac{m^4(\log m)^3}{k}\right).$$

Proof. Roughly speaking, by the upper bound for exponential sum

$$\left|\sum_{l=\frac{m+1}{2}}^{m-1} e_m(-al)\right| \leq \frac{m}{2|a|}, \qquad \text{where} \qquad 1 \leq |a| \leq \frac{m-1}{2}, \tag{2.4}$$

we know that only the terms when $|a_1|, |a_2|, |a_3|, |a_4|$ all are small contribute significantly to the main term in $\Xi_{m,k}$. Furthermore, for small enough $|a_1|, |a_2|, |a_3|, |a_4|$ the system of congruence equations

$$\begin{cases} a_1+a_2+a_3+a_4 \equiv 0 \pmod m, \\ a_2+2a_3+3a_4 \equiv 0 \pmod k, \end{cases}$$

is just a system of equations

$$\begin{cases} a_1+a_2+a_3+a_4 = 0, \\ a_2+2a_3+3a_4 = 0. \end{cases}$$

Specifically, for absolute constant $c > 0$ we get from (2.4) that

$$\sum_{ck\leq|a_1|\leq\frac{m-1}{2}} \sum_{\substack{1\leq|a_2|,|a_3|,|a_4|\leq\frac{m-1}{2} \\ a_1+a_2+a_3+a_4\equiv 0 \pmod m}} \left|\sum_{l_1=\frac{m+1}{2}}^{m-1} e_m(-a_1l_1)\right| \cdot \left|\sum_{l_2=\frac{m+1}{2}}^{m-1} e_m(-a_2l_2)\right|$$

$$\times \left| \sum_{l_3=\frac{m+1}{2}}^{m-1} e_m(-a_3 l_3) \right| \cdot \left| \sum_{l_4=\frac{m+1}{2}}^{m-1} e_m(-a_4 l_4) \right|$$

$$\ll \sum_{1\le|a_2|\le\frac{m-1}{2}} \frac{m}{|a_2|} \sum_{1\le|a_3|\le\frac{m-1}{2}} \frac{m}{|a_3|} \sum_{1\le|a_4|\le\frac{m-1}{2}} \frac{m}{|a_4|} \sum_{\substack{ck\le|a_1|\le\frac{m-1}{2} \\ a_1+a_2+a_3+a_4\equiv 0 \pmod m}} \frac{m}{k}$$

$$\ll \frac{m^4(\log m)^3}{k}.$$

By applying the above $\ll$ estimate directly to each of a_1, a_2, a_3, a_4 sequentially we have

$$\begin{aligned}
\Xi_{m,k} &= \sum_{1\le|a_1|,|a_2|\le\frac{5k}{32}} \sum_{\substack{1\le|a_3|,|a_4|\le\frac{k}{32} \\ a_1+a_2+a_3+a_4\equiv 0 \pmod m \\ a_2+2a_3+3a_4\equiv 0 \pmod k}} \sum_{l_1=\frac{m+1}{2}}^{m-1} e_m(-a_1 l_1) \sum_{l_2=\frac{m+1}{2}}^{m-1} e_m(-a_2 l_2) \\
&\quad \times \sum_{l_3=\frac{m+1}{2}}^{m-1} e_m(-a_3 l_3) \sum_{l_4=\frac{m+1}{2}}^{m-1} e_m(-a_4 l_4) + O\left(\frac{m^4(\log m)^3}{k}\right) \\
&= \sum_{1\le|a_1|,|a_2|\le\frac{5k}{32}} \sum_{\substack{1\le|a_3|,|a_4|\le\frac{k}{32} \\ a_1+a_2+a_3+a_4=0 \\ a_2+2a_3+3a_4=0}} \sum_{l_1=\frac{m+1}{2}}^{m-1} e_m(-a_1 l_1) \sum_{l_2=\frac{m+1}{2}}^{m-1} e_m(-a_2 l_2) \\
&\quad \times \sum_{l_3=\frac{m+1}{2}}^{m-1} e_m(-a_3 l_3) \sum_{l_4=\frac{m+1}{2}}^{m-1} e_m(-a_4 l_4) + O\left(\frac{m^4(\log m)^3}{k}\right) \\
&= \sum_{1\le|a_3|,|a_4|\le\frac{k}{32}} \sum_{l_1=\frac{m+1}{2}}^{m-1} e_m(-(a_3+2a_4) l_1) \sum_{l_2=\frac{m+1}{2}}^{m-1} e_m((2a_3+3a_4) l_2) \\
&\quad \times \sum_{l_3=\frac{m+1}{2}}^{m-1} e_m(-a_3 l_3) \sum_{l_4=\frac{m+1}{2}}^{m-1} e_m(-a_4 l_4) + O\left(\frac{m^4(\log m)^3}{k}\right).
\end{aligned}$$

It is not hard to show from (2.4) that

$$\begin{aligned}
&\sum_{\frac{k}{32}<|a_3|\le\frac{m-1}{2}} \sum_{1\le|a_4|\le\frac{k}{32}} \sum_{l_1=\frac{m+1}{2}}^{m-1} e_m(-(a_3+2a_4) l_1) \sum_{l_2=\frac{m+1}{2}}^{m-1} e_m((2a_3+3a_4) l_2) \\
&\quad \times \sum_{l_3=\frac{m+1}{2}}^{m-1} e_m(-a_3 l_3) \sum_{l_4=\frac{m+1}{2}}^{m-1} e_m(-a_4 l_4) \\
&\ll \sum_{\frac{k}{32}<|a_3|\le\frac{m-1}{2}} \sum_{1\le|a_4|\le\frac{k}{32}} m \cdot \left| \sum_{l_2=\frac{m+1}{2}}^{m-1} e_m((2a_3+3a_4) l_2) \right| \cdot \frac{m}{|a_3|} \cdot \frac{m}{|a_4|}
\end{aligned}$$

$$\begin{aligned}
&\ll \frac{m^3}{k} \sum_{1\le|a_4|\le\frac{k}{32}} \frac{1}{|a_4|} \sum_{\frac{k}{32}<|a_3|\le\frac{m-1}{2}} \left| \sum_{l_2=\frac{m+1}{2}}^{m-1} e_m\left((2a_3+3a_4)l_2\right)\right| \\
&\le \frac{m^3}{k} \sum_{1\le|a_4|\le\frac{k}{32}} \frac{1}{|a_4|} \sum_{0\le|a_3|\le\frac{m-1}{2}} \left| \sum_{l_2=\frac{m+1}{2}}^{m-1} e_m\left((2a_3+3a_4)l_2\right)\right| \\
&= \frac{m^3}{k} \sum_{1\le|a_4|\le\frac{k}{32}} \frac{1}{|a_4|} \sum_{0\le|a_3|\le\frac{m-1}{2}} \left| \sum_{l_2=\frac{m+1}{2}}^{m-1} e_m\left(a_3 l_2\right)\right| \\
&\ll \frac{m^3}{k}\cdot\log k\cdot m\log m \ll \frac{m^4(\log m)^2}{k},
\end{aligned}$$

where we used the trivial bound $\left|\sum\limits_{l_1=\frac{m+1}{2}}^{m-1} e_m\left(-(a_3+2a_4)l_1\right)\right| \ll m$. By applying the above $\ll$ estimate to each of a_3, a_4 sequentially we have

$$\begin{aligned}
\Xi_{m,k} &= \sum_{1\le|a_3|,|a_4|\le\frac{m-1}{2}} \sum_{l_1=\frac{m+1}{2}}^{m-1} e_m\left(-(a_3+2a_4)l_1\right) \sum_{l_2=\frac{m+1}{2}}^{m-1} e_m\left((2a_3+3a_4)l_2\right) \\
&\quad\times \sum_{l_3=\frac{m+1}{2}}^{m-1} e_m\left(-a_3 l_3\right) \sum_{l_4=\frac{m+1}{2}}^{m-1} e_m\left(-a_4 l_4\right) + O\left(\frac{m^4(\log m)^3}{k}\right) \\
&= \sum_{\frac{m+1}{2}\le l_1,l_2,l_3,l_4\le m-1} \sum_{1\le|a_3|\le\frac{m-1}{2}} e_m\left((-l_1+2l_2-l_3)a_3\right) \\
&\quad\times \sum_{1\le|a_4|\le\frac{m-1}{2}} e_m\left((-2l_1+3l_2-l_4)a_4\right) + O\left(\frac{m^4(\log m)^3}{k}\right) \\
&= \sum_{\frac{m+1}{2}\le l_1,l_2,l_3,l_4\le m-1} \sum_{0\le|a_3|\le\frac{m-1}{2}} e_m\left((-l_1+2l_2-l_3)a_3\right) \\
&\quad\times \sum_{0\le|a_4|\le\frac{m-1}{2}} e_m\left((-2l_1+3l_2-l_4)a_4\right) \\
&\quad- \sum_{\frac{m+1}{2}\le l_1,l_2,l_3,l_4\le m-1} \sum_{0\le|a_3|\le\frac{m-1}{2}} e_m\left((-l_1+2l_2-l_3)a_3\right) \\
&\quad- \sum_{\frac{m+1}{2}\le l_1,l_2,l_3,l_4\le m-1} \sum_{0\le|a_4|\le\frac{m-1}{2}} e_m\left((-2l_1+3l_2-l_4)a_4\right) \\
&\quad+ \sum_{\frac{m+1}{2}\le l_1,l_2,l_3,l_4\le m-1} 1 + O\left(\frac{m^4(\log m)^3}{k}\right) \\
&= m^2 \sum_{\substack{\frac{m+1}{2}\le l_1,l_2,l_3,l_4\le m-1 \\ 2l_2\equiv l_1+l_3 (\bmod m) \\ 3l_2\equiv 2l_1+l_4 (\bmod m)}} 1 - \frac{m(m-1)}{2} \sum_{\substack{\frac{m+1}{2}\le l_1,l_2,l_3\le m-1 \\ 2l_2\equiv l_1+l_3 (\bmod m)}} 1
\end{aligned}$$

$$-\frac{m(m-1)}{2}\sum_{\substack{\frac{m+1}{2}\le l_1,l_2,l_4\le m-1\\ 3l_2\equiv 2l_1+l_4(\bmod m)}}1+\frac{(m-1)^4}{16}$$
$$+O\left(\frac{m^4(\log m)^3}{k}\right), \tag{2.5}$$

where we used (2.3) in the last equality.

Following the same arguments in Lemma 2.2 of [15] we have

$$\begin{aligned}\sum_{\substack{\frac{m+1}{2}\le l_1,l_2,l_3\le m-1\\ 2l_2\equiv l_1+l_3(\bmod m)}}1 &= \sum_{\substack{1\le u_1,u_2,u_3\le\frac{m-1}{2}\\ 2(u_2+\frac{m-1}{2})\equiv u_1+\frac{m-1}{2}+u_3+\frac{m-1}{2}(\bmod m)}}1=\sum_{\substack{1\le u_1,u_2,u_3\le\frac{m-1}{2}\\ 2u_2\equiv u_1+u_3(\bmod m)}}1\\ &=\sum_{\substack{1\le u_1,u_2,u_3\le\frac{m-1}{2}\\ 2u_2=u_1+u_3}}1=\sum_{\substack{1\le u_1,u_3\le\frac{m-1}{2}\\ 2\mid u_1+u_3}}1=\sum_{1\le u_1\le\frac{m-1}{2}}\left(\frac{m}{4}+O(1)\right)\\ &=\frac{m^2}{8}+O(m)\end{aligned} \tag{2.6}$$

and

$$\begin{aligned}\sum_{\substack{\frac{m+1}{2}\le l_1,l_2,l_4\le m-1\\ 3l_2\equiv 2l_1+l_4(\bmod m)}}1 &= \sum_{\substack{1\le u_1,u_2,u_4\le\frac{m-1}{2}\\ 3(u_2+\frac{m-1}{2})\equiv 2(u_1+\frac{m-1}{2})+u_4+\frac{m-1}{2}(\bmod m)}}1=\sum_{\substack{1\le u_1,u_2,u_4\le\frac{m-1}{2}\\ 2u_1\equiv 3u_2-u_4(\bmod m)}}1\\ &=\sum_{\substack{1\le u_1,u_2,u_4\le\frac{m-1}{2}\\ 3-\frac{m-1}{2}\le 3u_2-u_4\le 0\\ 2u_1=3u_2-u_4+m}}1+\sum_{\substack{1\le u_1,u_2,u_4\le\frac{m-1}{2}\\ 1\le 3u_2-u_4\le m\\ 2u_1=3u_2-u_4}}1+\sum_{\substack{1\le u_1,u_2,u_4\le\frac{m-1}{2}\\ m+1\le 3u_2-u_4\le\frac{3(m-1)}{2}-1\\ 2u_1=3u_2-u_4-m}}1\\ &=\sum_{\substack{1\le u_2,u_4\le\frac{m-1}{2}\\ 3-\frac{m-1}{2}\le 3u_2-u_4\le 0\\ 2\mid 3u_2-u_4+m}}1+\sum_{\substack{1\le u_2,u_4\le\frac{m-1}{2}\\ 1\le 3u_2-u_4\le m\\ 2\mid 3u_2-u_4}}1+\sum_{\substack{1\le u_2,u_4\le\frac{m-1}{2}\\ m+1\le 3u_2-u_4\le\frac{3(m-1)}{2}-1\\ 2\mid 3u_2-u_4-m}}1\\ &=\sum_{\substack{1\le u_2,u_4\le\frac{m-1}{2}\\ 3u_2\le u_4\\ 2\nmid 3u_2-u_4}}1+\sum_{\substack{1\le u_2,u_4\le\frac{m-1}{2}\\ u_4+1\le 3u_2\le u_4+m\\ 2\mid 3u_2-u_4}}1+\sum_{\substack{1\le u_2,u_4\le\frac{m-1}{2}\\ u_4+m+1\le 3u_2\le\frac{3(m-1)}{2}+u_4-1\\ 2\nmid 3u_2-u_4}}1.\end{aligned}$$

By elementary calculations we get

$$\sum_{\substack{1\le u_2,u_4\le\frac{m-1}{2}\\ 3u_2\le u_4\\ 2\nmid 3u_2-u_4}}1=\sum_{1\le u_4\le\frac{m-1}{2}}\sum_{\substack{1\le u_2\le\frac{1}{3}u_4\\ 2\nmid 3u_2-u_4}}1=\sum_{1\le u_4\le\frac{m-1}{2}}\left(\frac{1}{6}u_4+O(1)\right)=\frac{1}{48}m^2+O(m),$$

$$\sum_{\substack{1\le u_2,u_4\le\frac{m-1}{2}\\ u_4+1\le 3u_2\le u_4+m\\ 2\mid 3u_2-u_4}}1=\sum_{1\le u_4\le\frac{m-1}{2}}\sum_{\substack{\frac{u_4+1}{3}\le u_2\le\frac{u_4+m}{3}\\ 2\mid 3u_2-u_4}}1=\sum_{1\le u_4\le\frac{m-1}{2}}\left(\frac{m}{6}+O(1)\right)=\frac{1}{12}m^2+O(m),$$

$$\sum_{\substack{1\le u_2,u_4\le\frac{m-1}{2}\\ u_4+m+1\le 3u_2\le\frac{3(m-1)}{2}+u_4-1\\ 2\nmid 3u_2-u_4}} 1 = \sum_{1\le u_4\le\frac{m-1}{2}} \sum_{\substack{\frac{u_4+m+1}{3}\le u_2\le\frac{m-1}{2}\\ 2\nmid 3u_2-u_4}} 1 = \sum_{1\le u_4\le\frac{m-1}{2}} \left(\frac{m}{12}-\frac{u_4}{6}+O(1)\right) = \frac{1}{48}m^2+O(m).$$

Hence,

$$\sum_{\substack{\frac{m+1}{2}\le l_1,l_2,l_4\le m-1\\ 3l_2\equiv 2l_1+l_4(\bmod m)}} 1 = \frac{1}{48}m^2+\frac{1}{12}m^2+\frac{1}{48}m^2+O(m) = \frac{1}{8}m^2+O(m). \tag{2.7}$$

Furthermore, we have

$$\begin{aligned}\sum_{\substack{\frac{m+1}{2}\le l_1,l_2,l_3,l_4\le m-1\\ 2l_2\equiv l_1+l_3(\bmod m)\\ 3l_2\equiv 2l_1+l_4(\bmod m)}} 1 &= \sum_{\substack{1\le u_1,u_2,u_3,u_4\le\frac{m-1}{2}\\ 2(u_2+\frac{m-1}{2})\equiv u_1+\frac{m-1}{2}+u_3+\frac{m-1}{2}(\bmod m)\\ 3(u_2+\frac{m-1}{2})\equiv 2(u_1+\frac{m-1}{2})+u_4+\frac{m-1}{2}(\bmod m)}} 1 = \sum_{\substack{1\le u_1,u_2,u_3,u_4\le\frac{m-1}{2}\\ 2u_2\equiv u_1+u_3(\bmod m)\\ 3u_2\equiv 2u_1+u_4(\bmod m)}} 1\\ &= \sum_{\substack{1\le u_1,u_2,u_3,u_4\le\frac{m-1}{2}\\ 2u_2=u_1+u_3\\ 6u_2\equiv 4u_1+2u_4(\bmod m)}} 1 = \sum_{\substack{1\le u_1,u_3,u_4\le\frac{m-1}{2}\\ 2\mid u_1+u_3\\ 3u_3-u_1\equiv 2u_4(\bmod m)}} 1.\end{aligned}$$

For $1\le u_1,u_3,u_4\le\frac{m-1}{2}$ with $2\mid u_1+u_3$, we know that

$$\begin{aligned}&-\frac{m-1}{2}+3\le 3u_3-u_1\le\frac{3(m-1)}{2}-1,\quad 2\mid 3u_3-u_1,\\ &1\le 2u_4\le m-1,\quad 2\mid 2u_4.\end{aligned}$$

Then $3u_3-u_1\equiv 2u_4\pmod m \Longleftrightarrow 3u_3-u_1=2u_4$. Hence,

$$\begin{aligned}\sum_{\substack{\frac{m+1}{2}\le l_1,l_2,l_3,l_4\le m-1\\ 2l_2\equiv l_1+l_3(\bmod m)\\ 3l_2\equiv 2l_1+l_4(\bmod m)}} 1 &= \sum_{\substack{1\le u_1,u_3,u_4\le\frac{m-1}{2}\\ 2\mid u_1+u_3\\ 3u_3-u_1=2u_4}} 1 = \sum_{\substack{1\le u_1,u_3\le\frac{m-1}{2}\\ 2\mid u_1+u_3\\ 1\le 3u_3-u_1\le m-1}} 1 = \sum_{\substack{1\le u_1,u_3\le\frac{m-1}{2}\\ 2\mid u_1+u_3\\ u_1+1\le 3u_3\le u_1+m-1}} 1\\ &= \sum_{1\le u_1\le\frac{m-1}{2}} \sum_{\substack{\frac{u_1+1}{3}\le u_3\le\frac{u_1+m-1}{3}\\ 2\mid u_1+u_3}} 1 = \sum_{1\le u_1\le\frac{m-1}{2}} \left(\frac{m}{6}+O(1)\right)\\ &= \frac{1}{12}m^2+O(m).\end{aligned} \tag{2.8}$$

Combining (2.5)–(2.8) we immediately get

$$\begin{aligned}\Xi_{m,k} &= m^2\left(\frac{m^2}{12}+O(m)\right)-2\cdot\frac{m(m-1)}{2}\left(\frac{m^2}{8}+O(m)\right)+\frac{(m-1)^4}{16}\\ &\quad +O\left(\frac{m^4(\log m)^3}{k}\right)\\ &= \frac{1}{48}m^4+O\left(\frac{m^4(\log m)^3}{k}\right).\end{aligned}$$

This completes the proof of Lemma 2.2. □

3. Correlation measures of order 4

Now we prove Theorem 1.1. By the orthogonality relations of additive character sums we get

$$s_t = \frac{1}{m} \sum_{|a| \le \frac{m-1}{2}} \sum_{l=\frac{m+1}{2}}^{m-1} e_m\left(a(Q_m(t) - l)\right).$$

Hence,

$$(-1)^{s_t} = 1 - 2s_t = -\frac{2}{m} \sum_{1 \le |a| \le \frac{m-1}{2}} \sum_{l=\frac{m+1}{2}}^{m-1} e_m(-al)\, e_m(aQ_m(t)) + \frac{1}{m}.$$

Define

$$\chi_{km}(n) = \begin{cases} e_m(Q_m(n)), & \text{if } \gcd(n, m) = 1, \\ 0, & \text{if } \gcd(n, m) > 1. \end{cases}$$

Following from the assumption that $Q_m(n)$ is km-periodic we get $\chi_{km}(n + km) = \chi_{km}(n)$, and by (1.1) we have

$$\chi_{km}(n_1 n_2) = \chi_{km}(n_1)\chi_{km}(n_2).$$

Then $\chi_{km}(n)$ is a Dirichlet character modulo km such that χ_{km}^m is trivial and $\chi_{km}^{m'}$ is not trivial for all $1 \le m' < m$. Therefore

$$(-1)^{s_t} = -\frac{2}{m} \sum_{1 \le |a| \le \frac{m-1}{2}} \sum_{l=\frac{m+1}{2}}^{m-1} e_m(-al)\, \chi_{km}(t^a) + \frac{1}{m}. \tag{3.1}$$

By (2.4) we get

$$\begin{aligned} &\left| -\frac{2}{m} \sum_{1 \le |a| \le \frac{m-1}{2}} \sum_{l=\frac{m+1}{2}}^{m-1} e_m(-al)\, \chi_{km}(t^a) \right| \le \frac{2}{m} \sum_{1 \le |a| \le \frac{m-1}{2}} \left| \sum_{l=\frac{m+1}{2}}^{m-1} e_m(-al) \right| \\ &\le \frac{2}{m} \sum_{1 \le |a| \le \frac{m-1}{2}} \frac{m}{2|a|} \ll \log m. \end{aligned} \tag{3.2}$$

Then from (3.1) and (3.2) we have

$$\begin{aligned} \sum_{t=0}^{km-1} (-1)^{s_t + s_{t+m} + s_{t+2m} + s_{t+3m}} &= \sum_{\substack{t=0 \\ \gcd(t,m)=1}}^{km-1} (-1)^{s_t + s_{t+m} + s_{t+2m} + s_{t+3m}} + \sum_{\substack{t=0 \\ \gcd(t,m)>1}}^{km-1} 1 \\ = \sum_{\substack{t=0 \\ \gcd(t,m)=1}}^{km-1} &\left(-\frac{2}{m} \sum_{1 \le |a_1| \le \frac{m-1}{2}} \sum_{l_1=\frac{m+1}{2}}^{m-1} e_m(-a_1 l_1)\, \chi_{km}(t^{a_1}) + \frac{1}{m} \right) \\ &\times \left(-\frac{2}{m} \sum_{1 \le |a_2| \le \frac{m-1}{2}} \sum_{l_2=\frac{m+1}{2}}^{m-1} e_m(-a_2 l_2)\, \chi_{km}((t+m)^{a_2}) + \frac{1}{m} \right) \end{aligned}$$

$$\times\Big(-\frac{2}{m}\sum_{1\le|a_3|\le\frac{m-1}{2}}\sum_{l_3=\frac{m+1}{2}}^{m-1}e_m(-a_3l_3)\chi_{km}((t+2m)^{a_3})+\frac{1}{m}\Big)$$

$$\times\Big(-\frac{2}{m}\sum_{1\le|a_4|\le\frac{m-1}{2}}\sum_{l_4=\frac{m+1}{2}}^{m-1}e_m(-a_4l_4)\chi_{km}((t+3m)^{a_4})+\frac{1}{m}\Big)+\sum_{\substack{t=0\\ \gcd(t,m)>1}}^{km-1}1$$

$$=\frac{2^4}{m^4}\sum_{1\le|a_1|\le\frac{m-1}{2}}\sum_{l_1=\frac{m+1}{2}}^{m-1}e_m(-a_1l_1)\sum_{1\le|a_2|\le\frac{m-1}{2}}\sum_{l_2=\frac{m+1}{2}}^{m-1}e_m(-a_2l_2)$$

$$\times\sum_{1\le|a_3|\le\frac{m-1}{2}}\sum_{l_3=\frac{m+1}{2}}^{m-1}e_m(-a_3l_3)\sum_{1\le|a_4|\le\frac{m-1}{2}}\sum_{l_4=\frac{m+1}{2}}^{m-1}e_m(-a_4l_4)$$

$$\times\sum_{t=0}^{km-1}\chi_{km}(t^{a_1}(t+m)^{a_2}(t+2m)^{a_3}(t+3m)^{a_4})$$

$$+\sum_{\substack{t=0\\ \gcd(t,m)>1}}^{km-1}1+O\Big(k(\log m)^3\Big). \tag{3.3}$$

Combining (2.4), (3.3), Lemmas 2.1 and 2.2 we get

$$\sum_{t=0}^{km-1}(-1)^{s_t+s_{t+m}+s_{t+2m}+s_{t+3m}}$$

$$=\frac{2^4k\phi(m)}{m^4}\sum_{\substack{1\le|a_1|,|a_2|,|a_3|,|a_4|\le\frac{m-1}{2}\\ a_1+a_2+a_3+a_4\equiv0\ (\mathrm{mod}\ m)\\ a_2+2a_3+3a_4\equiv0\ (\mathrm{mod}\ k)}}\sum_{l_1=\frac{m+1}{2}}^{m-1}e_m(-a_1l_1)\sum_{l_2=\frac{m+1}{2}}^{m-1}e_m(-a_2l_2)$$

$$\times\sum_{l_3=\frac{m+1}{2}}^{m-1}e_m(-a_3l_3)\sum_{l_4=\frac{m+1}{2}}^{m-1}e_m(-a_4l_4)$$

$$+O\Bigg(\frac{1}{m^4}\Bigg(\sum_{1\le|a|\le\frac{m-1}{2}}\Bigg|\sum_{l=\frac{m+1}{2}}^{m-1}e_m(-al)\Bigg|\Bigg)^4\phi(m)\phi(k)^{-1}k^{\frac{3}{2}}\Bigg)$$

$$+\sum_{\substack{t=0\\ \gcd(t,m)>1}}^{km-1}1+O\Big(k(\log m)^3\Big)$$

$$=km-\frac{2}{3}k\phi(m)+O\Big(k^{\frac{1}{2}}m(\log m)^4\Big).$$

Then there exists absolute constant $\delta>0$ such that

$$\sum_{t=0}^{km-1}(-1)^{s_t+s_{t+m}+s_{t+2m}+s_{t+3m}}\ge\frac{1}{3}km-\delta k^{\frac{1}{2}}m(\log m)^4.$$

This proves the result.

4. Final remarks

In this work, we have claimed that two families of binary sequences (see (1.3) and (1.4)) studied in the past several years have 'large' values on the correlation measures of order 4. They would be very vulnerable if used in cryptography.

It seems interesting to consider the case when the full peaks on the periodic correlation measure of these sequences appear, i.e., their periodic correlation measure of order ℓ equals to the period, see [9]. Such problem may be related to their linear complexity.

Acknowledgments

H. Liu was partially supported by National Natural Science Foundation of China under Grant No. 12071368, and the Science and Technology Program of Shaanxi Province of China under Grant No. 2019JM-573 and 2020JM-026.

Z. Chen and C. Wu were partially supported by the Provincial Natural Science Foundation of Fujian under grant No. 2020J01905, by the Science and Technology Project of Putian City under grant No. 2021R4001-10, and by the Putian Univ. under grant No. PTU-P-61772292.

Conflict of interest

The authors declared that they have no conflicts of interest to this work.

References

1. T. Agoh, K. Dilcher, L. Skula, Fermat quotients for composite moduli, *J. Number Theory*, **66** (1997), 29–50. https://doi.org/10.1006/jnth.1997.2162
2. H. Aly, A. Winterhof, Boolean functions derived from Fermat quotients, *Cryptogr. Commun.*, **3** (2011), 165–174. https://doi.org/10.1007/s12095-011-0043-5
3. T. Apostol, *Introduction to analytic number theory*, New York: Springer, 1976. https://doi.org/10.1007/978-1-4757-5579-4
4. J. Cassaigne, C. Mauduit, A. Sárközy, On finite pseudorandom binary sequences vii: the measures of pseudorandomness, *Acta Arith.*, **103** (2002), 97–118. https://doi.org/10.4064/aa103-2-1
5. M. Chang, Short character sums with Fermat quotients, *Acta Arith.*, **152** (2012), 23–38. https://doi.org/10.4064/aa152-1-3
6. Z. Chen, Trace representation and linear complexity of binary sequences derived from Fermat quotients, *Sci. China Inf. Sci.*, **57** (2014), 1–10. https://doi.org/10.1007/s11432-014-5092-x
7. Z. Chen, X. Du, On the linear complexity of binary threshold sequences derived from Fermat quotients, *Des. Codes Cryptogr.*, **67** (2013), 317–323. https://doi.org/10.1007/s10623-012-9608-3
8. Z. Chen, X. Du, R. Marzouk, Trace representation of pseudorandom binary sequences derived from Euler quotients, *Appl. Algebra Eng. Commun. Comput.*, **26** (2015), 555–570. https://doi.org/10.1007/s00200-015-0265-4

9. Z. Chen, A. Gómez, D. Gómez-Pérez, A. Tirkel, Correlation measure, linear complexity and maximum order complexity for families of binary sequences, *Finite Fields Th. Appl.*, **78** (2022), 101977. https://doi.org/10.1016/j.ffa.2021.101977
10. Z. Chen, L. Hu, X. Du, Linear complexity of some binary sequences derived from Fermat quotients, *China Commun.*, **9** (2012), 105–108. https://doi.org/10.1007/s11277-010-0104-7
11. Z. Chen, A. Ostafe, A. Winterhof, Structure of pseudorandom numbers derived from Fermat quotients, In: *Lecture notes in computer science*, Berlin: Springer, 2010, 73–85. https://doi.org/10.1007/978-3-642-13797-6_6
12. Z. Chen, A. Winterhof, Interpolation of Fermat quotients, *SIAM J. Discrete Math.*, **28** (2014), 1–7. https://doi.org/10.1137/130907951
13. X. Du, Z. Chen, L. Hu, Linear complexity of binary sequences derived from Euler quotients with prime-power modulus, *Inform. Process. Lett.*, **112** (2012), 604–609. https://doi.org/10.1016/j.ipl.2012.04.011
14. D. Gómez-Pérez, A. Winterhof, Multiplicative character sums of Fermat quotients and pseudorandom sequences, *Period. Math. Hung.*, **64** (2012), 161–168. https://doi.org/10.1007/s10998-012-3747-1
15. H. Liu, X. Liu, On the correlation measures of orders 3 and 4 of binary sequence of period p^2 derived from Fermat quotients, *Adv. Math. Commun.*, in press. https://doi.org/10.3934/amc.2021008
16. C. Mauduit, A. Sárközy, On finite pseudorandom binary sequencs I: measure of pseudorandomness, the Legendre symbol, *Acta Arith.*, **82** (1997), 365–377. https://doi.org/10.4064/aa-82-4-365-377
17. A. Ostafe, I. Shparlinski, Pseudorandomness and dynamics of Fermat quotients, *SIAM J. Discrete Math.*, **25** (2011), 50–71. https://doi.org/10.1137/100798466
18. C. D. Pan, C. B. Pan, *Goldbach conjecture (Chinese)*, Beijing: Science Press, 2011.
19. I. Shparlinski, Fermat quotients: exponential sums, value set and primitive roots, *Bull. Lond. Math. Soc.*, **43** (2011), 1228–1238. https://doi.org/10.1112/blms/bdr058
20. I. Shparlinski, Character sums with Fermat quotients, *Q. J. Math.*, **62** (2011), 1031–1043. https://doi.org/10.1093/qmath/haq028
21. I. Shparlinski, Bounds of multiplicative character sums with Fermat quotients of primes, *Bull. Aust. Math. Soc.*, **83** (2011), 456–462. https://doi.org/10.1017/S000497271000198X
22. J. Zhang, S. Gao, C. Zhao, Linear complexity of a family of binary pq^2-periodic sequences from Euler quotients, *IEEE Trans. Inf. Theory*, **66** (2020), 5774–5780. https://doi.org/10.1109/TIT.2020.2979838
23. J. Zhang, C. Hu, X. Fan, C. Zhao, Trace representation of the binary pq^2-periodic sequences derived from Euler quotients, *Cryptogr. Commun.*, **13** (2021), 343–359. https://doi.org/10.1007/s12095-021-00475-1

AIMS Press

© 2022 the Author(s), licensee AIMS Press. This is an open access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0)