Publ. Math. Debrecen
79/1-2 (2011), 145–170
DOI: 10.5486/PMD.2011.4997

On the correlation of pseudorandom binary sequences using additive characters

By HUANING LIU (Xi'an) and XIAOYUN WANG (Jinan)

Abstract. In this paper we study the correlation of pseudorandom binary sequences using additive characters, and study the number of quadruples in two special subsets in $\mathbb{Z}_p$.

1. 1. Introduction

Pseudorandom binary sequences play an important role in cryptography, so in a series of papers a new constructive approach has been developed to study the pseudorandomness of the binary sequences

$$E_N = (e_1, \dots, e_N) \in \{-1, +1\}^N .$$

In particular in [9] C. MAUDUIT and A. SÁRKÖZY first introduced the following measures of pseudorandomness: the *well-distribution measure* of E_N is defined by

$$W(E_N) = \max_{a,b,t} \left| \sum_{j=0}^{t-1} e_{a+jb} \right| ,$$

where the maximum is taken over all a, b, $t \in \mathbb{N}$ with $1 \le a \le a + (t-1)b \le N$. The *correlation measure of order* k of E_N is denoted as

$$C_k(E_N) = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \dots e_{n+d_k} \right| ,$$

Mathematics Subject Classification: 11K45.
Key words and phrases: pseudorandom binary sequence; additive character; subset.
This paper is supported by the National Natural Science Foundation of China under Grant No. 10901128; and the Natural Science Foundation of the Education Department of Shaanxi Province of China under Grant No. 09JK762.

where the maximum is taken over all $D = (d_1, \dots, d_k)$ and M with $0 \le d_1 < \cdots < d_k \le N - M$, and the *combined (well-distribution-correlation) PR- measure of order k*

$$Q_k(E_N) = \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \cdots e_{a+jb+d_k} \right|$$

is defined for all a, b, t, $D = (d_1, \dots, d_k)$ with $1 \le a+jb+d_i \le N$ $(i = 1, 2, \dots, k)$.

The sequence is considered as a "good" pseudorandom sequence if both $W(E_N)$ and $C_k(E_N)$ (at least for small k) are "small" in terms of N. Later many pseudorandom binary sequences were given and studied (see [1], [4], [6], [7], [12], [13], [8], [10], [11] for details). For example, let p be an odd prime number, $f(x) \in \mathbb{F}_p[x]$, and define $E_p = (e_1, \dots, e_p)$ by

$$e_n = \begin{cases} +1, & \text{if} \quad 0 \le R_p(f(n)) < p/2, \\ -1, & \text{if} \quad p/2 \le R_p(f(n)) < p, \end{cases} \tag{1.1}$$

where $R_p(n)$ denotes the unique $r \in \{0, 1, \dots, p-1\}$ such that $n \equiv r \pmod p$. C. Mauduit, J. Rivat and A. Sárközy [8] studied the sequence (1.1). They showed that for this sequence both $W(E_N)$ and the correlations of "small" order are "small":

Proposition 1.1. *For $f \in \mathbb{F}_p[x]$ of degree d and $E_p = (e_1, \dots, e_p)$ defined by* (1.1)*, we have*

$$W(E_p) \ll dp^{1/2}(\log p)^2.$$

Proposition 1.2. *For $f \in \mathbb{F}_p[x]$ of degree d and $E_p = (e_1, \dots, e_p)$ defined by* (1.1)*, we have for $2 \le l \le d-1$,*

$$C_l(E_p) \ll dp^{1/2}(\log p)^{l+1}.$$

On the other hand, they showed that certain correlations of "large" order can be "large":

Proposition 1.3. *For any $k = 2^t$ there exists a constant $c = c(k) > 0$ such that if p is a prime number large enough, $f \in \mathbb{F}_p[x]$ is of degree k and $E_p = (e_1, \dots, e_p)$ is defined by* (1.1)*, then*

$$\max_{\substack{T,M \\ 1 \le T < T+M \le p}} \left| \sum_{n=T}^{T+M} e_n e_{n+1} \dots e_{n+k-1} \right| \gg cp.$$

In this paper we shall further study the correlation of sequence (1.1). In Section 3 we show that for this sequence the correlations of odd order are "small":

Theorem 1.1. *For $f \in \mathbb{F}_p[x]$ of degree $d \geq 2$ and $E_p = (e_1, \ldots, e_p)$ defined by* (1.1)*, we have for $l \in \mathbb{N}$ with $2 \nmid l$,*

$$C_l(E_p) \ll dp^{1/2}(\log p)^{l+1}.$$

In [8] C. Mauduit, J. Rivat and A. Sárközy wrote that,"we expect that if the order of the correlation is greater than the degree of the polynomial, then the correlation is large. However, this can not be shown along these lines since then there are many large terms contributing to the sum to be estimated, thus a different approach is needed." In Section 4 we shall give a simple example to show that this conjecture may be true.

Theorem 1.2. *Let $p > 3$ be a prime, and let $E'_p = (e'_1, \ldots, e'_p)$ be defined by*

$$e'_n = \begin{cases} +1, & \text{if} \quad 0 \leq R_p(n^3) < p/2, \\ -1, & \text{if} \quad p/2 \leq R_p(n^3) < p. \end{cases} \tag{1.2}$$

Then for any M with $M \ll \frac{p}{(\log p)^4}$, we have

$$\sum_{n \leq M} e'_n e'_{n+1} e'_{n+2} e'_{n+3} \gg M.$$

The famous Szemerédi's theorem asserts that any set of integers of positive upper density contains arbitrarily long arithmetic progressions. E. Szemerédi [16], [17] used combinatorial methods to give the first full proof of this theorem. Later, H. Furstenberg [2], [3] introduced an ergodic theoretic proof of this theorem. K. F. Roth [14] proved Szemerédi's theorem for progressions of length three by using the exponential sums. His proof could be concluded as follows.

(1) Define an appropriate notion of pseudorandomness.

(2) Prove that every pseudorandom subset of $\{1, 2, \ldots, N\}$ contains roughly the number of arithmetic progressions of length k that you would expect.

(3) Prove that if $A \subset \{1, 2, \ldots, N\}$ has size δN and is not pseudorandom, then there exists an arithmetic progression $P \subset \{1, 2, \ldots, N\}$ with length tending to infinite with N, such that $|A \cap P| \geq (\delta + \epsilon)|P|$, for some $\epsilon > 0$ that depends on δ and k only.

W. T. Gowers [5] generalized Roth's argument. Let $\mathbb{Z}_N$ be the ring of integers modulo N. For $f : \mathbb{Z}_N \to \mathbb{C}$ and any k, the difference function $\Delta(f;k)$ is defined by $\Delta(f;k)(s) = f(s)\overline{f(s-k)}$, and the iterated difference function $\Delta(f;a_1,\dots,a_d)$ is denoted by

$$\Delta(f;a_1,\dots,a_d)(s) = \Delta(\Delta(f;a_1,\dots,a_{d-1});a_d)(s).$$

Furthermore we set $\hat{f}(r) = \sum_{s\in\mathbf{Z}_N} f(s)\mathrm{e}\big(-\frac{rs}{N}\big)$, where $\mathrm{e}(y) = \mathrm{e}^{2\pi iy}$, and $\hat{f}$ is the discrete Fourier transform of f. Let A be a subset of $\mathbb{Z}_N$, and denote the characteristic function of A by the same letter. Given a set A of cardinality δN, we define the balanced function of A to be $f_A : \mathbf{Z}_N \to [-1,+1]$, where

$$f_A(s) = \begin{cases} 1-\delta, & s \in A, \\ -\delta, & s \notin A. \end{cases}$$

It is easy to show that $\hat{f}_A(r) = \hat{A}(r)$ for $r \neq 0$.

Definition 1.1. Let D denote the closed unit disc in $\mathbb{C}$, and $f : \mathbb{Z}_N \to D$. If there are at most $o(N^{d-1})$ values of $(a_1,\dots,a_{d-1})$ for which there exists some $r \in \mathbb{Z}_N$ with

$$\Big|\widehat{\Delta(f;a_1,\dots,a_{d-1})}(r)\Big| \gg N,$$

we say that f is uniform of degree d. If f is the balanced function f_A of some set $A \subset \mathbb{Z}_N$, then we shall also say that A is uniform of degree d. Especially when d equals one or two, we say that f is uniform or quadratically uniform.

W. T. Gowers [5] proved the following:

Proposition 1.4. *Let $A \subset \mathbb{Z}_N$ be uniform of degree $k-2$ and have cardinality δN. Then A contains an arithmetic progression of length k.*

Furthermore, he presented the following conjecture.

Conjecture 1.1. *Let $A \subset \mathbb{Z}_N$ be a set of size δN. Then, if A is uniform, the number of quadruples $(x, x+d, x+2d, x+3d)$ in A^4 is at least $(\delta^4-\alpha)N^2$, where $\alpha = o(\delta)$.*

In Section 5 we shall study two special subsets of $\mathbb{Z}_N$, and prove the following results.

Theorem 1.3. *Let $A_1 = \{n : n \in \mathbb{Z}_p, 0 \le R_p(n^3) < p/2\}$. Then A_1 is quadratic uniform. Let $A_1 = \delta p$, then $\delta = \frac{1}{2} + O\big(\frac{1}{p^{1/2}\log p}\big)$ and*

$$\sum_{d\le p}\sum_{n\le p} A_1(n)A_1(n+d)A_1(n+2d)A_1(n+3d) = \delta^4p^2 + O\left(p^{3/2}(\log p)^4\right).$$

Theorem 1.4. *Let* $A_2 = \{n : n \in \mathbb{Z}_p, 0 \le R_p(n^2) < p/2\}$. *Then* A_2 *is uniform, but* A_2 *is not quadratic uniform. Let* $A_2 = \delta p$, *then*

$$\delta = \frac{1}{2} + O\left(\frac{1}{p^{1/2}\log p}\right)$$

and

$$\sum_{d\le p}\sum_{n\le p} A_2(n)A_2(n+d)A_2(n+2d)A_2(n+3d) = \left(\delta^4 + \frac{1}{8192}\right)p^2 + O\left(p^{3/2}(\log p)^4\right).$$

2. Some lemmas

To prove the theorems, we need the following lemmas.

Lemma 2.1. *If* $n \in \mathbb{Z}$ *and* m *is an odd integer, then we have*

$$\frac{1}{m}\sum_{|a|<m/2} v_m(a)\mathrm{e}\left(\frac{an}{m}\right) = \begin{cases} +1, & \text{if } \ 0 \le R_m(n) < m/2, \\ -1, & \text{if } \ m/2 \le R_m(n) < m, \end{cases}$$

where $v_m(a)$ *is a function of period* m *such that*

$$v_m(0) = 1, \quad v_m(a) = 1 + i\frac{(-1)^a - \cos(\pi a/m)}{\sin(\pi a/m)} \quad (1 \le |a| < m/2).$$

Furthermore, $v_m(a)$ *satisfies*

$$v_m(a) = \begin{cases} O(1), & \text{if } a \text{ is even}, \\ -\dfrac{2im}{\pi a} + O(1), & \text{if } a \text{ is odd}. \end{cases}$$

Proof. This is Lemma 2 in [8]. □

Lemma 2.2. *For any polynomial* $f(x)$ *of* $\mathbb{F}_p[x]$ *of degree* $d \ge 2$ *and any integers* M *and* K *with* $1 \le K < p$ *we have*

$$\left|\sum_{n=M+1}^{M+K} \mathrm{e}\left(\frac{f(n)}{p}\right)\right| \ll dp^{1/2}\log p.$$

Proof. See [18]. □

Lemma 2.3. *Suppose that p is a prime number and $f(x) = a_l x^l + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ is a polynomial with $0 < l < p$ and $(a_l, p) = 1$. Then*

$$\left| \sum_{n=0}^{p-1} \mathrm{e}\left(\frac{f(n)}{p}\right) \right| \le (l-1)\, p^{1/2}.$$

PROOF. This is Corollary 2F in [15]. □

Lemma 2.4. *Let $p > 3$ be a prime, and let j, k be integers with $0 \le j < k \le 3$. Then we have*

$$\Psi_1 := \sum_{|a_j|<p/2} \sum_{|a_k|<p/2} v_p(a_j) v_p(a_k) \sum_{d \le p-1} \sum_{n \le p} \mathrm{e}\left(\frac{a_j(n+jd)^3 + a_k(n+kd)^3}{p}\right)$$
$$\ll p^{7/2} (\log p)^2.$$

PROOF. Let $G_1(n) = a_j(n+jd)^3 + a_k(n+kd)^3$. Then

$$\Psi_1 = \sum_{|a_j|<p/2} \sum_{|a_k|<p/2} v_p(a_j) v_p(a_k) \sum_{d \le p-1} \sum_{\substack{n \le p \\ \deg(G_1(n)) \ge 2}} \mathrm{e}\left(\frac{G_1(n)}{p}\right)$$
$$+ \sum_{|a_j|<p/2} \sum_{|a_k|<p/2} v_p(a_j) v_p(a_k) \sum_{d \le p-1} \sum_{\substack{n \le p \\ \deg(G_1(n)) \le 1}} \mathrm{e}\left(\frac{G_1(n)}{p}\right) := \sum\nolimits_1 + \sum\nolimits_2.$$

By Lemma 2.1 and Lemma 2.3 we easily get

$$\sum\nolimits_1 \ll \sum_{|a_j|<p/2} \sum_{|a_k|<p/2} |v_p(a_j)|\, |v_p(a_k)| \sum_{d \le p-1} p^{1/2}$$
$$\ll p^{3/2} \left(\sum_{\substack{|a|<p/2 \\ a \ne 0}} \frac{p}{|a|} \right)^2 \ll p^{7/2} (\log p)^2.$$

On the other hand, noting that

$$G_1(n) = (a_j + a_k) n^3 + 3dn^2 (j a_j + k a_k) + 3d^2 n (j^2 a_j + k^2 a_k) + d^3 (j^3 a_j + k^3 a_k),$$

then

$$\deg(G_1(n) \le 1 \quad \text{if and only if} \quad \begin{cases} a_j + a_k \equiv 0 \pmod p \\ j a_j + k a_k \equiv 0 \pmod p, \end{cases}$$

which implies that $a_j = a_k = 0$. Then we have

$$\sum\nolimits_2 \ll v_p(0)v_p(0)p^2 \ll p^2.$$

Therefore

$$\Psi_1 \ll p^{7/2}(\log p)^2. \qquad \square$$

Lemma 2.5. *Let $p > 3$ be a prime, and let j, k, l be integers with $0 \le j < k < l \le 3$. Then we have*

$$\begin{aligned}\Psi_2 &:= \sum_{|a_j|<p/2} \sum_{|a_k|<p/2} \sum_{|a_l|<p/2} v_p(a_j)v_p(a_k)v_p(a_l) \\ &\quad \times \sum_{d\le p-1} \sum_{n\le p} \mathrm{e}\left(\frac{a_j(n+jd)^3 + a_k(n+kd)^3 + a_l(n+ld)^3}{p}\right) \\ &\ll p^{9/2}(\log p)^3.\end{aligned}$$

Proof. Let $G_2(n) = a_j(n+jd)^3 + a_k(n+kd)^3 + a_l(n+ld)^3$. Then

$$\begin{aligned}\Psi_2 &= \sum_{|a_j|<p/2} \sum_{|a_k|<p/2} \sum_{|a_l|<p/2} v_p(a_j)v_p(a_k)v_p(a_l) \sum_{d\le p-1} \sum_{\substack{n\le p \\ \deg(G_2(n))\ge 2}} \mathrm{e}\left(\frac{G_2(n)}{p}\right) \\ &\quad + \sum_{|a_j|<p/2} \sum_{|a_k|<p/2} \sum_{|a_l|<p/2} v_p(a_j)v_p(a_k)v_p(a_l) \sum_{d\le p-1} \sum_{\substack{n\le p \\ \deg(G_2(n))\le 1}} \mathrm{e}\left(\frac{G_2(n)}{p}\right) \\ &:= \sum\nolimits_1 + \sum\nolimits_2. \end{aligned} \tag{2.1}$$

By Lemma 2.1 and Lemma 2.3 we easily get

$$\begin{aligned}\sum\nolimits_1 &\ll \sum_{|a_j|<p/2} \sum_{|a_k|<p/2} \sum_{|a_l|<p/2} |v_p(a_j)|\,|v_p(a_k)|\,|v_p(a_l)| \sum_{d\le p-1} p^{1/2} \\ &\ll p^{3/2}\Bigg(\sum_{\substack{|a|<p/2 \\ a\ne 0}} \frac{p}{|a|}\Bigg)^3 \ll p^{9/2}(\log p)^3. \end{aligned} \tag{2.2}$$

On the other hand, noting that

$$\begin{aligned}G_2(n) &= (a_j + a_k + a_l)n^3 + 3dn^2(ja_j + ka_k + la_l) \\ &\quad + 3d^2n(j^2a_j + k^2a_k + l^2a_l) + d^3(j^3a_j + k^3a_k + l^3a_l),\end{aligned}$$

then

$$\deg(G_2(n)\le 1 \quad \text{if and only if} \quad \begin{cases} a_j+a_k+a_l\equiv 0 \pmod p\\ ja_j+ka_k+la_l\equiv 0 \pmod p. \end{cases}$$

Therefore

$$\begin{aligned}\sum\nolimits_2 &= \sum_{\substack{|a_j|<p/2\\ a_j+a_k+a_l\equiv 0 \pmod p\\ ja_j+ka_k+la_l\equiv 0 \pmod p}} \sum_{|a_k|<p/2} \sum_{|a_l|<p/2} v_p(a_j)v_p(a_k)v_p(a_l)\\ &\quad\times \sum_{d\le p-1}\sum_{n\le p} \mathrm{e}\left(\frac{3d^2n(j^2a_j+k^2a_k+l^2a_l)+d^3(j^3a_j+k^3a_k+l^3a_l)}{p}\right)\\ &= p\sum_{\substack{|a_j|<p/2\\ a_j+a_k+a_l\equiv 0 \pmod p\\ ja_j+ka_k+la_l\equiv 0 \pmod p\\ j^2a_j+k^2a_k+l^2a_l\equiv 0 \pmod p}} \sum_{|a_k|<p/2} \sum_{|a_l|<p/2} v_p(a_j)v_p(a_k)v_p(a_l)\\ &\quad\times \sum_{d\le p-1} \mathrm{e}\left(\frac{d^3(j^3a_j+k^3a_k+l^3a_l)}{p}\right).\end{aligned}$$

Since

$$\begin{cases} a_j+a_k+a_l\equiv 0 \pmod p\\ ja_j+ka_k+la_l\equiv 0 \pmod p\\ j^2a_j+k^2a_k+l^2a_l\equiv 0 \pmod p \end{cases} \quad \text{if and only if} \quad \begin{cases} a_j\equiv 0 \pmod p\\ a_k\equiv 0 \pmod p\\ a_l\equiv 0 \pmod p, \end{cases}$$

we have

$$\sum\nolimits_2 \ll p^2. \tag{2.3}$$

Now from (2.1)-(2.3) we immediately get

$$\Psi_2 \ll p^{9/2}(\log p)^3. \qquad \square$$

Lemma 2.6. *Let $p>3$ be a prime. Then we have*

$$\begin{aligned}\Psi_3 &:= \sum_{|a_0|<p/2} \sum_{|a_1|<p/2} \sum_{|a_2|<p/2} \sum_{|a_3|<p/2} v_p(a_0)v_p(a_1)v_p(a_2)v_p(a_3)\\ &\quad\times \sum_{d\le p-1}\sum_{n\le p} \mathrm{e}\left(\frac{a_0n^3+a_1(n+d)^3+a_2(n+2d)^3+a_3(n+3d)^3}{p}\right)\\ &\ll p^{11/2}(\log p)^4.\end{aligned}$$

PROOF. Let $G_3(n) = a_0n^3 + a_1(n+d)^3 + a_2(n+2d)^3 + a_3(n+3d)^3$. Then

$$\begin{aligned}\Psi_3 &= \sum_{|a_0|<p/2}\sum_{|a_1|<p/2}\sum_{|a_2|<p/2}\sum_{|a_3|<p/2} v_p(a_0)v_p(a_1)v_p(a_2)v_p(a_3)\\ &\quad\times \sum_{d\le p-1}\sum_{\substack{n\le p\\ \deg(G_3(n))\ge 2}} \mathrm{e}\left(\frac{G_3(n)}{p}\right)\\ &\quad+ \sum_{|a_0|<p/2}\sum_{|a_1|<p/2}\sum_{|a_2|<p/2}\sum_{|a_3|<p/2} v_p(a_0)v_p(a_1)v_p(a_2)v_p(a_3)\\ &\quad\times \sum_{d\le p-1}\sum_{\substack{n\le p\\ \deg(G_3(n))\le 1}} \mathrm{e}\left(\frac{G_3(n)}{p}\right) = \sum\nolimits_1 + \sum\nolimits_2. \end{aligned} \tag{2.4}$$

By Lemma 2.1 and Lemma 2.3 we easily get

$$\begin{aligned}\sum\nolimits_1 &\ll \sum_{|a_0|<p/2}\sum_{|a_1|<p/2}\sum_{|a_2|<p/2}\sum_{|a_3|<p/2} |v_p(a_0)||v_p(a_1)||v_p(a_2)||v_p(a_3)| \sum_{d\le p-1} p^{1/2}\\ &\ll p^{3/2}\left(\sum_{\substack{|a|<p/2\\ a\ne 0}} \frac{p}{|a|}\right)^4 \ll p^{11/2}(\log p)^5. \end{aligned} \tag{2.5}$$

Noting that

$$\begin{aligned}G_3(n) &= (a_0+a_1+a_2+a_3)n^3 + 3dn^2(a_1+2a_2+3a_3)\\ &\quad + 3d^2n(a_1+4a_2+9a_3) + d^3(a_1+8a_2+27a_3),\end{aligned}$$

then

$$\deg(G_3(n)) \le 1 \quad \text{if and only if} \quad \begin{cases} a_0+a_1+a_2+a_3 \equiv 0 \pmod p\\ a_1+2a_2+3a_3 \equiv 0 \pmod p.\end{cases}$$

Therefore

$$\begin{aligned}\sum\nolimits_2 &= \sum_{\substack{|a_0|<p/2\\ a_0+a_1+a_2+a_3\equiv 0 \pmod p\\ a_1+2a_2+3a_3\equiv 0 \pmod p}}\sum_{|a_1|<p/2}\sum_{|a_2|<p/2}\sum_{|a_3|<p/2} v_p(a_0)v_p(a_1)v_p(a_2)v_p(a_3)\\ &\quad\times \sum_{d\le p-1}\sum_{n\le p} \mathrm{e}\left(\frac{3d^2n(a_1+4a_2+9a_3)+d^3(a_1+8a_2+27a_3)}{p}\right)\end{aligned}$$

$$= p \sum_{\substack{|a_0|<p/2 \\ a_0+a_1+a_2+a_3\equiv 0 \pmod p \\ a_1+2a_2+3a_3\equiv 0 \pmod p \\ a_1+4a_2+9a_3\equiv 0 \pmod p}} \sum_{|a_1|<p/2} \sum_{|a_2|<p/2} \sum_{|a_3|<p/2} v_p(a_0)v_p(a_1)v_p(a_2)v_p(a_3)$$
$$\times \sum_{d\le p-1} \mathrm{e}\left(\frac{d^3(a_1+8a_2+27a_3)}{p}\right).$$

By Lemma 2.1 and Lemma 2.3 we can get

$$\begin{aligned}\sum\nolimits_2 &\ll p \sum_{\substack{|a_0|<p/2 \\ a_0+a_1+a_2+a_3\equiv 0 \pmod p \\ a_1+2a_2+3a_3\equiv 0 \pmod p \\ a_1+4a_2+9a_3\equiv 0 \pmod p \\ a_1+8a_2+27a_3\not\equiv 0 \pmod p}} \sum_{|a_1|<p/2} \sum_{|a_2|<p/2} \sum_{|a_3|<p/2} |v_p(a_0)||v_p(a_1)||v_p(a_2)||v_p(a_3)| \cdot p^{1/2} \\ &+ p(p-1) \sum_{\substack{|a_0|<p/2 \\ a_0+a_1+a_2+a_3\equiv 0 \pmod p \\ a_1+2a_2+3a_3\equiv 0 \pmod p \\ a_1+4a_2+9a_3\equiv 0 \pmod p \\ a_1+8a_2+27a_3\equiv 0 \pmod p}} \sum_{|a_1|<p/2} \sum_{|a_2|<p/2} \sum_{|a_3|<p/2} |v_p(a_0)||v_p(a_1)||v_p(a_2)||v_p(a_3)| \\ &\ll p^{3/2}\left(\sum_{\substack{|a|<p/2 \\ a\ne 0}} \frac{p}{|a|}\right)^4 + p(p-1)|v_p(0)|^4 \ll p^{11/2}(\log p)^4. \end{aligned} \tag{2.6}$$

Then from (2.4)-(2.6) we immediately have

$$\Psi_3 \ll p^{11/2}(\log p)^5. \qquad \square$$

Lemma 2.7. *Let $p > 3$ be a prime, and let j, k be integers with $0 \le j < k \le 3$. Then we have*

$$\begin{aligned}\Upsilon_1 &:= \sum_{|a_j|<p/2} q, \sum_{|a_k|<p/2} v_p(a_j)v_p(a_k) \sum_{d\le p-1} \sum_{n\le p} \mathrm{e}\left(\frac{a_j(n+jd)^2 + a_k(n+kd)^2}{p}\right) \\ &\ll p^{7/2}(\log p)^2.\end{aligned}$$

Proof. By Lemma 2.1 and Lemma 2.3 we easily get

$$\Upsilon_1 = \sum_{\substack{|a_j|<p/2 \\ p|a_j+a_k}} \sum_{|a_k|<p/2} v_p(a_j)v_p(a_k) \sum_{d\le p-1} \sum_{n\le p} \mathrm{e}\left(\frac{a_j(n+jd)^2 + a_k(n+kd)^2}{p}\right)$$

$$+ O\Bigg(\sum_{\substack{|a_j|<p/2 \\ p\nmid a_j+a_k}} \sum_{|a_k|<p/2} |v_p(a_j)||v_p(a_k)| \cdot p^{3/2} \Bigg)$$

$$= \sum_{\substack{|a|<p/2 \\ a\neq 0}} v_p(a)v_p(-a) \sum_{d\le p-1} \sum_{n\le p} \mathrm{e}\left(\frac{2ad(j-k)n + ad^2(j^2-k^2)}{p} \right)$$

$$+ O\left(p^{7/2}(\log p)^2 \right) \ll p^{7/2}(\log p)^2. \qquad \square$$

Lemma 2.8. *Let $p > 3$ be a prime, and let j, k, l be integers with $0 \le j < k < l \le 3$. Then we have*

$$\Upsilon_2 := \sum_{|a_j|<p/2} \sum_{|a_k|<p/2} \sum_{|a_l|<p/2} v_p(a_j)v_p(a_k)v_p(a_l)$$
$$\times \sum_{d\le p-1} \sum_{n\le p} e\left(\frac{a_j(n+jd)^2 + a_k(n+kd)^2 + a_l(n+ld)^2}{p} \right) \ll p^{9/2}(\log p)^3.$$

Proof. By Lemma 2.1 and Lemma 2.3 we get

$$\Upsilon_2 = \sum_{\substack{|a_j|<p/2 \\ a_j+a_k+a_l\equiv 0 \pmod p}} \sum_{|a_k|<p/2} \sum_{|a_l|<p/2} v_p(a_j)v_p(a_k)v_p(a_l)$$
$$\times \sum_{d\le p-1} \sum_{n\le p} \mathrm{e}\left(\frac{a_j(n+jd)^2 + a_k(n+kd)^2 + a_l(n+ld)^2}{p} \right)$$
$$+ O\Bigg(\sum_{\substack{|a_j|<p/2 \\ a_j+a_k+a_l\not\equiv 0 \pmod p}} \sum_{|a_k|<p/2} \sum_{|a_l|<p/2} |v_p(a_j)||v_p(a_k)||v_p(a_l)| \cdot p^{3/2} \Bigg)$$

$$= \sum_{\substack{|a_j|<p/2 \\ a_j+a_k+a_l\equiv 0 \pmod p}} \sum_{|a_k|<p/2} \sum_{|a_l|<p/2} v_p(a_j)v_p(a_k)v_p(a_l)$$
$$\times \sum_{d\le p-1} \sum_{n\le p} \mathrm{e}\left(\frac{2d(ja_j + ka_k + la_l)n + d^2(j^2a_j + k^2a_k + l^2a_l)}{p} \right)$$
$$+ O\left(p^{9/2}(\log p)^3 \right)$$

$$= p \sum_{\substack{|a_j|<p/2 \\ a_j+a_k+a_l\equiv 0 \pmod p \\ ja_j+ka_k+la_l\equiv 0 \pmod p}} \sum_{|a_k|<p/2} \sum_{|a_l|<p/2} v_p(a_j)v_p(a_k)v_p(a_l) \sum_{d\le p-1} \mathrm{e}\left(\frac{d^2(j^2a_j+k^2a_k+l^2a_l)}{p} \right)$$

$$
\begin{aligned}
&+O\left(p^{9/2}(\log p)^3\right)\\
&=p(p-1)\sum_{\substack{|a_j|<p/2\\ a_j+a_k+a_l\equiv 0 \pmod p\\ ja_j+ka_k+la_l\equiv 0 \pmod p\\ j^2a_j+k^2a_k+l^2a_l\equiv 0 \pmod p}}\sum_{|a_k|<p/2}\sum_{|a_l|<p/2} v_p(a_j)v_p(a_k)v_p(a_l)\\
&+O\left(p\sum_{\substack{|a_j|<p/2\\ a_j+a_k+a_l\equiv 0 \pmod p\\ ja_j+ka_k+la_l\equiv 0 \pmod p\\ j^2a_j+k^2a_k+l^2a_l\not\equiv 0 \pmod p}}\sum_{|a_k|<p/2}\sum_{|a_l|<p/2} |v_p(a_j)||v_p(a_k)||v_p(a_l)|\cdot p^{1/2}\right)\\
&+O\left(p^{9/2}(\log p)^3\right)\\
&=p(p-1)\sum_{\substack{|a_j|<p/2\\ a_j+a_k+a_l\equiv 0 \pmod p\\ ja_j+ka_k+la_l\equiv 0 \pmod p\\ j^2a_j+k^2a_k+l^2a_l\equiv 0 \pmod p}}\sum_{|a_k|<p/2}\sum_{|a_l|<p/2} v_p(a_j)v_p(a_k)v_p(a_l)+O\left(p^{9/2}(\log p)^3\right).
\end{aligned}
$$

Noting that

$$
\begin{cases} a_j+a_k+a_l\equiv 0 \pmod p\\ ja_j+ka_k+la_l\equiv 0 \pmod p\\ j^2a_j+k^2a_k+l^2a_l\equiv 0 \pmod p \end{cases}
\quad\text{if and only if}\quad
\begin{cases} a_j\equiv 0 \pmod p\\ a_k\equiv 0 \pmod p\\ a_l\equiv 0 \pmod p, \end{cases}
$$

then we have

$$\Upsilon_2\ll p^{9/2}(\log p)^3. \qquad \square$$

Lemma 2.9. *Let $p>3$ be a prime. Then we have*

$$
\begin{aligned}
\Upsilon_3:=&\sum_{|a_0|<p/2}\sum_{|a_1|<p/2}\sum_{|a_2|<p/2}\sum_{|a_3|<p/2} v_p(a_0)v_p(a_1)v_p(a_2)v_p(a_3)\\
&\times\sum_{d\le p-1}\sum_{n\le p} e\left(\frac{a_0n^2+a_1(n+d)^2+a_2(n+2d)^2+a_3(n+3d)^2}{p}\right)\\
=&\frac{1}{512}p^6+O\left(p^{11/2}(\log p)^4\right).
\end{aligned}
$$

PROOF. By using the methods in Lemma 2.8 we can get

$$\Upsilon_3 = p(p-1) \sum_{\substack{|a_0|<p/2 \\ a_0+a_1+a_2+a_3\equiv 0 \pmod p \\ a_1+2a_2+3a_3\equiv 0 \pmod p \\ a_1+4a_2+9a_3\equiv 0 \pmod p}} \sum_{|a_1|<p/2} \sum_{|a_2|<p/2} \sum_{|a_3|<p/2} v_p(a_j)v_p(a_k)v_p(a_l)$$

$$+ O\left(p^{11/2}(\log p)^4\right).$$

Noting that

$$\begin{cases} a_0+a_1+a_2+a_3 \equiv 0 \pmod p \\ a_1+2a_2+3a_3 \equiv 0 \pmod p \\ a_1+4a_2+9a_3 \equiv 0 \pmod p \end{cases} \quad \text{if and only if} \quad \begin{cases} a_0 \equiv -a_3 \pmod p \\ a_1 \equiv 3a_3 \pmod p \\ a_2 \equiv -3a_3 \pmod p, \end{cases}$$

therefore

$$\Upsilon_3 = p(p-1) \sum_{|a|<p/2} v_p(-a)v_p(3a)v_p(-3a)v_p(a) + O\left(p^{11/2}(\log p)^4\right).$$

It is not hard to show that

$$\sum_{p/6\le|a|<p/2} v_p(-a)v_p(3a)v_p(-3a)v_p(a) \ll \sum_{p/6\le|a|<p/2} \frac{p^4}{|a|^4} \ll p$$

and

$$\sum_{\substack{|a|<p/2 \\ 2|a}} v_p(-a)v_p(3a)v_p(-3a)v_p(a) \ll \sum_{\substack{|a|<p/2 \\ 2|a}} 1 \ll p,$$

then from Lemma 2.1 we have

$$\begin{aligned}
\Upsilon_3 &= p(p-1) \sum_{\substack{|a|<p/6 \\ 2\nmid a}} v_p(-a)v_p(3a)v_p(-3a)v_p(a) + O\left(p^{11/2}(\log p)^4\right) \\
&= p(p-1) \sum_{\substack{|a|<p/6 \\ 2\nmid a}} \left(\frac{2ip}{\pi a} + O(1)\right)\left(-\frac{2ip}{3\pi a} + O(1)\right) \\
&\quad \times \left(\frac{2ip}{3\pi a} + O(1)\right)\left(-\frac{2ip}{\pi a} + O(1)\right) + O\left(p^{11/2}(\log p)^4\right) \\
&= \frac{1}{9\pi^4}p^5(p-1) \sum_{\substack{|a|<p/6 \\ 2\nmid a}} \frac{1}{a^4} + O\left(p^{11/2}(\log p)^4\right) \\
&= \frac{5\zeta(4)}{24\pi^4}p^6 + O\left(p^{11/2}(\log p)^4\right) = \frac{1}{512}p^6 + O\left(p^{11/2}(\log p)^4\right). \qquad \square
\end{aligned}$$

3. Proof of Theorem 1.1

For $M < p$, $l \in \mathbb{N}$ with $2 \nmid l$, and $0 \le d_1 < \cdots < d_l \le p - M$, from Lemma 2.1 we have

$$\begin{aligned}
&\sum_{n\le M} e_{n+d_1}\cdots e_{n+d_l}\\
&= \frac{1}{p^l}\sum_{|a_1|<p/2}\cdots\sum_{|a_l|<p/2} v_p(a_1)\ldots v_p(a_l)\sum_{n\le M}\mathrm{e}\left(\frac{a_1f(n+d_1)+\cdots+a_lf(n+d_l)}{p}\right)\\
&= \frac{1}{p^l}\sum_{\substack{|a_1|<p/2\\ p\nmid a_1+\cdots+a_l}}\cdots\sum_{|a_l|<p/2} v_p(a_1)\ldots v_p(a_l)\sum_{n\le M}\mathrm{e}\left(\frac{a_1f(n+d_1)+\cdots+a_lf(n+d_l)}{p}\right)\\
&\quad+\frac{1}{p^l}\sum_{\substack{|a_1|<p/2\\ p\mid a_1+\cdots+a_l}}\cdots\sum_{|a_l|<p/2} v_p(a_1)\ldots v_p(a_l)\sum_{n\le M}\mathrm{e}\left(\frac{a_1f(n+d_1)+\cdots+a_lf(n+d_l)}{p}\right)\\
&:= \sum\nolimits_1+\sum\nolimits_2. \qquad (3.1)
\end{aligned}$$

Suppose that a is the leading coefficient of $f(n)$, then $a(a_1+\cdots+a_l)$ is the leading coefficient of $a_1f(n+d_1)+\cdots+a_lf(n+d_l)$. If $p\nmid a_1+\cdots+a_l$, then the degree of $a_1f(n+d_1)+\cdots+a_lf(n+d_l)$ is ≥ 2. So from Lemma 2.2 and Lemma 2.1 we get

$$\begin{aligned}
\sum\nolimits_1 &\ll \frac{1}{p^l}\sum_{\substack{|a_1|<p/2\\ p\nmid a_1+\cdots+a_l}}\cdots\sum_{|a_l|<p/2}|v_p(a_1)|\ldots|v_p(a_l)|\cdot dp^{1/2}\log p\\
&\ll dp^{1/2}\log p\cdot\frac{1}{p^l}\left(\sum_{\substack{|a|<p/2\\ a\ne 0}}\frac{p}{|a|}\right)^l \ll dp^{1/2}(\log p)^{l+1}. \qquad (3.2)
\end{aligned}$$

On the other hand, by Lemma 2.1 we can have

$$\begin{aligned}
&\sum_{\substack{|a_1|<p/2\\ 2\mid a_1}}\sum_{|a_2|<p/2}\cdots\sum_{|a_l|<p/2} v_p(a_1)v_p(a_2)\ldots v_p(a_l)\\
&\qquad\qquad\qquad\qquad p\mid a_1+a_2+\cdots+a_l\\
&\qquad\qquad\times\sum_{n\le M}\mathrm{e}\left(\frac{a_1f(n+d_1)+\cdots+a_lf(n+d_l)}{p}\right)\\
&\ll M\sum_{|a_2|<p/2}\cdots\sum_{|a_l|<p/2}|v_p(a_2)|\ldots|v_p(a_l)|
\end{aligned}$$

$$\ll M \cdot \left(\sum_{\substack{|a|<p/2 \\ a\neq 0}} \frac{p}{|a|} \right)^{l-1} \ll p^l (\log p)^{l-1}.$$

Therefore

$$\begin{aligned}
\sum\nolimits_2 &= \frac{1}{p^l} \sum_{\substack{|a_1|<p/2 \\ 2\nmid a_1 \\ p\mid a_1+\cdots+a_l}} \cdots \sum_{\substack{|a_l|<p/2 \\ 2\nmid a_l}} v_p(a_1)\ldots v_p(a_l) \\
&\quad \times \sum_{n\le M} \mathrm{e}\left(\frac{a_1 f(n+d_1)+\cdots+a_l f(n+d_l)}{p} \right) + O\left((\log p)^{l-1}\right) \\
&\ll M \sum_{\substack{|a_1|<p/2 \\ 2\nmid a_1 \\ p\mid a_1+\cdots+a_l}} \cdots \sum_{\substack{|a_l|<p/2 \\ 2\nmid a_l}} \frac{1}{|a_1\ldots a_l|} + (\log p)^{l-1} \\
&\ll p \sum_{\substack{|a_1|<p/2 \\ a_1\neq 0 \\ p\mid a_1+\cdots+a_l}} \cdots \sum_{\substack{|a_l|<p/2 \\ a_l\neq 0}} \frac{1}{|a_1\ldots a_l|} + (\log p)^{l-1}.
\end{aligned}$$

Noting that

$$\begin{aligned}
&\sum_{\substack{|a_1|<p/2 \\ a_1\neq 0 \\ p\mid a_1+\cdots+a_l \\ a_1+\cdots+a_l\neq 0}} \cdots \sum_{\substack{|a_l|<p/2 \\ a_l\neq 0}} \frac{1}{|a_1\ldots a_l|} \\
&= \sum_{\substack{|k|<l/2 \\ k\neq 0}} \sum_{\substack{|a_1|<p/2 \\ a_1\neq 0 \\ a_1+\cdots+a_l=kp}} \cdots \sum_{\substack{|a_l|<p/2 \\ a_l\neq 0}} \left| \frac{1}{a_1+\cdots+a_l} \left(\frac{1}{a_2\ldots a_l} + \cdots + \frac{1}{a_1\ldots a_{l-1}} \right) \right| \\
&= \sum_{\substack{|k|<l/2 \\ k\neq 0}} \frac{1}{|kp|} \sum_{\substack{|a_1|<p/2 \\ a_1\neq 0 \\ a_1+\cdots+a_l=kp}} \cdots \sum_{\substack{|a_l|<p/2 \\ a_l\neq 0}} \left| \frac{1}{a_2\ldots a_l} + \cdots + \frac{1}{a_1\ldots a_{l-1}} \right| \\
&\ll \frac{1}{p} \sum_{\substack{|k|<l/2 \\ k\neq 0}} \frac{1}{|k|} \cdot l \cdot \left(\sum_{\substack{|a|<p/2 \\ a\neq 0}} \frac{1}{|a|} \right)^{l-1} \ll \frac{1}{p} (\log p)^{l-1} \cdot l \log l,
\end{aligned}$$

we have

$$\sum\nolimits_2 \ll p \sum_{\substack{|a_1|<p/2\\ a_1\neq 0\\ a_1+\cdots+a_l=0}} \cdots \sum_{\substack{|a_l|<p/2\\ a_l\neq 0}} \frac{1}{|a_1\ldots a_l|} + (\log p)^{l-1}\cdot l\log l.$$

Since l, $a_1,\ldots,a_l$ are odd numbers, then $a_1+\cdots+a_l$ is odd. Therefore $a_1+\cdots+a_l=0$ is impossible. So we have

$$\sum\nolimits_2 \ll (\log p)^{l-1}\cdot l\log l. \tag{3.3}$$

Then from (3.1), (3.2) and (3.3) we get

$$\sum_{n\le M} e_{n+d_1}\ldots e_{n+d_l} \ll dp^{1/2}(\log p)^{l+1}.$$

Therefore

$$C_l(E_p) \ll dp^{1/2}(\log p)^{l+1}.$$

4. Proof of Theorem 1.2

By Lemma 2.1 we get

$$\begin{aligned}
&\sum_{n\le M} e'_n e'_{n+1} e'_{n+2} e'_{n+3}\\
&\quad = \frac{1}{p^4} \sum_{|a_0|<p/2} \sum_{|a_1|<p/2} \sum_{|a_2|<p/2} \sum_{|a_3|<p/2} v_p(a_0)v_p(a_1)v_p(a_2)v_p(a_3)\\
&\qquad \times \sum_{n\le M} \mathrm{e}\left(\frac{a_0n^3+a_1(n+1)^3+a_2(n+2)^3+a_3(n+3)^3}{p}\right).
\end{aligned}$$

Define $F(n)=a_0n^3+a_1(n+1)^3+a_2(n+2)^3+a_3(n+3)^3$. We have

$$\begin{aligned}
&\sum_{n\le M} e'_n e'_{n+1} e'_{n+2} e'_{n+3}\\
&\quad = \frac{1}{p^4} \sum_{|a_0|<p/2} \sum_{|a_1|<p/2} \sum_{|a_2|<p/2} \sum_{|a_3|<p/2} v_p(a_0)v_p(a_1)v_p(a_2)v_p(a_3)\\
&\qquad \times \sum_{\substack{n\le M\\ \deg(F(n))\ge 2}} \mathrm{e}\left(\frac{F(n)}{p}\right)
\end{aligned}$$

$$+\frac{1}{p^4}\sum_{|a_0|<p/2}\sum_{|a_1|<p/2}\sum_{|a_2|<p/2}\sum_{|a_3|<p/2} v_p(a_0)v_p(a_1)v_p(a_2)v_p(a_3)$$
$$\times \sum_{\substack{n\le M\\ \deg(F(n))\le 1}} \mathrm{e}\left(\frac{F(n)}{p}\right) = \Psi_1+\Psi_2. \tag{4.1}$$

By Lemma 2.1 and Lemma 2.2 we easily get

$$\Psi_1 \ll \frac{1}{p^4}\left(\sum_{\substack{|a|<p/2\\ a\neq 0}}\frac{p}{|a|}\right)^4 \cdot p^{1/2}\log p \ll p^{1/2}(\log p)^5. \tag{4.2}$$

On the other hand, noting that

$$F(n) = (a_0+a_1+a_2+a_3)n^3 + 3(a_1+2a_2+3a_3)n^2 + 3(a_1+4a_2+9a_3)n + (a_1+8a_2+27a_3).$$

Then

$$\deg(F(n))\le 1 \quad \text{if and only if} \quad \begin{cases} a_0+a_1+a_2+a_3 \equiv 0 \pmod p\\ a_1+2a_2+3a_3\equiv 0 \pmod p.\end{cases}$$

Therefore

$$\Psi_2 = \frac{1}{p^4}\sum_{\substack{|a_0|<p/2\\ a_0+a_1+a_2+a_3\equiv 0 \pmod p\\ a_1+2a_2+3a_3\equiv 0 \pmod p}}\sum_{|a_1|<p/2}\sum_{|a_2|<p/2}\sum_{|a_3|<p/2} v_p(a_0)v_p(a_1)v_p(a_2)v_p(a_3)$$
$$\times \sum_{n\le M} \mathrm{e}\left(\frac{6(a_2+3a_3)n+6(a_2+4a_3)}{p}\right).$$

Let $1\le A < \frac{p}{432M}$ be a parameter. We have

$$\sum_{\substack{A\le|a_0|<p/2\\ a_0+a_1+a_2+a_3\equiv 0 \pmod p\\ a_1+2a_2+3a_3\equiv 0 \pmod p}}\sum_{|a_1|<p/2}\sum_{|a_2|<p/2}\sum_{|a_3|<p/2} v_p(a_0)v_p(a_1)v_p(a_2)v_p(a_3)$$
$$\times \sum_{n\le M} \mathrm{e}\left(\frac{6(a_2+3a_3)n+6(a_2+4a_3)}{p}\right)$$

$$\ll \sum_{|a_1|<p/2} \sum_{|a_2|<p/2} \sum_{|a_3|<p/2} \frac{p}{A} |v_p(a_1)||v_p(a_2)||v_p(a_3)| \cdot M$$
$$\ll \frac{pM}{A} \left(\sum_{\substack{|a|<p/2 \\ a\neq 0}} \frac{p}{|a|} \right)^3 \ll \frac{p^4 M}{A} (\log p)^3 .$$

On the other hand,

$$\sum_{\substack{|a_0|<p/2 \\ 2|a_0 \\ a_0+a_1+a_2+a_3\equiv 0 \pmod p \\ a_1+2a_2+3a_3\equiv 0 \pmod p}} \sum_{|a_1|<p/2} \sum_{|a_2|<p/2} \sum_{|a_3|<p/2} v_p(a_0)v_p(a_1)v_p(a_2)v_p(a_3)$$
$$\times \sum_{n\le M} \mathrm{e}\left(\frac{6(a_2+3a_3)n + 6(a_2+4a_3)}{p} \right)$$
$$\ll \sum_{|a_1|<p/2} \sum_{|a_2|<p/2} \sum_{|a_3|<p/2} |v_p(a_1)||v_p(a_2)||v_p(a_3)| \cdot M$$
$$\ll M \left(\sum_{\substack{|a|<p/2 \\ a\neq 0}} \frac{p}{|a|} \right)^3 \ll p^3 M (\log p)^3 .$$

Therefore

$$\Psi_2 = \frac{1}{p^4} \sum_{\substack{|a_0|<A \\ 2\nmid a_0 \\ a_0+a_1+a_2+a_3\equiv 0 \pmod p \\ a_1+2a_2+3a_3\equiv 0 \pmod p}} \sum_{\substack{|a_1|<A \\ 2\nmid a_1}} \sum_{\substack{|a_2|<A \\ 2\nmid a_2}} \sum_{\substack{|a_3|<A \\ 2\nmid a_3}} v_p(a_0)v_p(a_1)v_p(a_2)v_p(a_3)$$
$$\times \sum_{n\le M} \mathrm{e}\left(\frac{6(a_2+3a_3)n + 6(a_2+4a_3)}{p} \right) + O\left(\frac{M}{A} (\log p)^3 \right)$$
$$= \frac{1}{p^4} \sum_{\substack{|a_2|<A \\ 2\nmid a_2}} \sum_{\substack{|a_3|<A \\ 2\nmid a_3}} v_p(a_2+3a_3)v_p(-2a_2-3a_3)v_p(a_2)v_p(a_3)$$
$$\times \sum_{n\le M} \mathrm{e}\left(\frac{6(a_2+3a_3)n + 6(a_2+4a_3)}{p} \right) + O\left(\frac{M}{A} (\log p)^3 \right)$$
$$= \frac{1}{p^4} \sum_{\substack{|a_2|<A \\ 2\nmid a_2}} \sum_{\substack{|a_3|<A \\ 2\nmid a_3}} \left(-\frac{2ip}{\pi(a_2+2a_3)} + O(1) \right) \left(\frac{2ip}{\pi(2a_2+3a_3)} + O(1) \right)$$

$$\times \left(-\frac{2ip}{\pi(a_2)}+O(1)\right)\left(-\frac{2ip}{\pi(a_3)}+O(1)\right)$$
$$\times \sum_{n\le M} \mathrm{e}\left(\frac{6(a_2+3a_3)n+6(a_2+4a_3)}{p}\right)+O\left(\frac{M}{A}(\log p)^3\right)$$
$$= -\frac{16}{\pi^4}\sum_{\substack{|a_2|<A\\ 2\nmid a_2}}\sum_{\substack{|a_3|<A\\ 2\nmid a_3}}\frac{1}{(a_2+2a_3)(2a_2+3a_3)a_2a_3}$$
$$\times \sum_{n\le M} \mathrm{e}\left(\frac{6(a_2+3a_3)n+6(a_2+4a_3)}{p}\right)+O\left(\frac{M}{A}(\log p)^3\right).$$

Since $|a_2|<A$, $|a_3|<A$ and $A<\frac{p}{432M}$, then

$$\frac{6(a_2+3a_3)n+6(a_2+4a_3)}{p}\le\frac{24MA+30A}{p}\le\frac{54MA}{p}\le\frac{1}{8}.$$

Therefore

$$\mathrm{Re}\sum_{n\le M}\mathrm{e}\left(\frac{6(a_2+3a_3)n+6(a_2+4a_3)}{p}\right)\gg M.$$

Then

$$|\Psi_2|\gg M\sum_{\substack{|a_2|<A\\ 2\nmid a_2}}\sum_{\substack{|a_3|<A\\ 2\nmid a_3}}\frac{1}{|a_2+2a_3||2a_2+3a_3||a_2||a_3|}+\frac{M}{A}(\log p)^3$$
$$\gg M+\frac{M}{A}(\log p)^3.$$

Noting that $M\ll\frac{p}{(\log p)^4}$, then we have

$$|\Psi_2|\gg M. \tag{4.3}$$

Then from (4.1), (4.2) and (4.3) we have

$$\sum_{n\le M}e'_ne'_{n+1}e'_{n+2}e'_{n+3}\gg M.$$

5. Proof of Theorem 1.3 and Theorem 1.4

First we prove Theorem 1.3. By Lemma 2.1 we get

$$A_1(n)=\frac{1}{2p}\sum_{|a|<p/2}v_p(a)\mathrm{e}\left(\frac{an^3}{p}\right)+\frac{1}{2}. \tag{5.1}$$

Then from Lemma 2.1 and Lemma 2.3 we get

$$|A_1| = \sum_{n=1}^{p} A_1(n) = \frac{1}{2p} \sum_{|a|<p/2} v_p(a) \sum_{n=1}^{p} \mathrm{e}\left(\frac{an^3}{p}\right) + \frac{p}{2}$$
$$= \frac{p}{2} + O\left(\frac{1}{p} \sum_{\substack{|a|<p/2 \\ a\neq 0}} \frac{p}{|a|} \cdot p^{1/2} + 1\right) = \frac{p}{2} + O\left(p^{1/2}\log p\right).$$

Define $|A_1| = \delta p$, then $\delta = \frac{1}{2} + O\big(\frac{1}{p^{1/2}\log p}\big)$.

For $r \neq 0$ and $k \neq 0$, by Lemma 2.1 and Lemma 2.3 we get

$$\widehat{\Delta(A_1;k)}(r) = \sum_{n=1}^{p} A_1(n)A_1(n-k)\mathrm{e}\left(-\frac{rn}{p}\right)$$
$$= \sum_{n=1}^{p} \left(\frac{1}{2p} \sum_{|a|<p/2} v_p(a)\mathrm{e}\left(\frac{an^3}{p}\right) + \frac{1}{2}\right)$$
$$\times \left(\frac{1}{2p} \sum_{|b|<p/2} v_p(b)\mathrm{e}\left(\frac{b(n-k)^3}{p}\right) + \frac{1}{2}\right) \mathrm{e}\left(-\frac{rn}{p}\right)$$
$$= \frac{1}{4p^2} \sum_{|a|<p/2} v_p(a) \sum_{|b|<p/2} v_p(b) \sum_{n=1}^{p} \mathrm{e}\left(\frac{an^3 + b(n-k)^3 - rn}{p}\right)$$
$$+ \frac{1}{4p} \sum_{|a|<p/2} v_p(a) \sum_{n=1}^{p} \mathrm{e}\left(\frac{an^3 - rn}{p}\right)$$
$$+ \frac{1}{4p} \sum_{|b|<p/2} v_p(b) \sum_{n=1}^{p} \mathrm{e}\left(\frac{b(n-k)^3 - rn}{p}\right)$$
$$+ \frac{1}{4} \sum_{n=1}^{p} \mathrm{e}\left(-\frac{rn}{p}\right)$$
$$= \frac{1}{4p^2} \sum_{|a|<p/2} v_p(a) \sum_{|b|<p/2} v_p(b) \sum_{n=1}^{p} \mathrm{e}\left(\frac{an^3 + b(n-k)^3 - rn}{p}\right)$$
$$+ O\left(\frac{1}{p} \sum_{\substack{|a|<p/2 \\ a\neq 0}} \frac{p}{|a|} \cdot p^{1/2}\right)$$
$$= \frac{1}{4p^2} \sum_{\substack{|a|<p/2 \\ p|a+b}} \sum_{|b|<p/2} v_p(a)v_p(b) \sum_{n=1}^{p} \mathrm{e}\left(\frac{an^3 + b(n-k)^3 - rn}{p}\right)$$

$$+ O\left(\frac{1}{p^2}\sum_{\substack{|a|<p/2\\ p\nmid a+b}}\sum_{|b|<p/2}|v_p(a)||v_p(b)|\cdot p^{1/2}\right) + O\left(p^{1/2}\log p\right)$$

$$= \frac{1}{4p^2}\sum_{|a|<p/2} v_p(a)v_p(-a)\sum_{n=1}^{p}\mathrm{e}\left(\frac{3kan^2-(3k^2a+r)n+ak^3}{p}\right)$$

$$+ O\left(p^{1/2}(\log p)^2\right)$$

$$\ll \frac{1}{p^2}\sum_{\substack{|a|<p/2\\ a\neq 0}}\frac{p^2}{a^2}\cdot p^{1/2} + p^{1/2}(\log p)^2 \ll p^{1/2}(\log p)^2.$$

Then A_1 is quadratically uniform according to Definition 1.1.

On the other hand, from (5.1) we have

$$\sum_{d\le p}\sum_{n\le p} A_1(n)A_1(n+d)A_1(n+2d)A_1(n+3d)$$

$$= \sum_{d\le p-1}\sum_{n\le p} A_1(n)A_1(n+d)A_1(n+2d)A_1(n+3d) + O(p)$$

$$= \sum_{d\le p-1}\sum_{n\le p}\left(\frac{1}{2}+\frac{1}{2p}\sum_{|a_0|<p/2} v_p(a_0)\mathrm{e}\left(\frac{a_0n^3}{p}\right)\right)$$

$$\times\left(\frac{1}{2}+\frac{1}{2p}\sum_{|a_1|<p/2} v_p(a_1)\mathrm{e}\left(\frac{a_1(n+d)^3}{p}\right)\right)$$

$$\times\left(\frac{1}{2}+\frac{1}{2p}\sum_{|a_2|<p/2} v_p(a_2)\mathrm{e}\left(\frac{a_2(n+2d)^3}{p}\right)\right)$$

$$\times\left(\frac{1}{2}+\frac{1}{2p}\sum_{|a_3|<p/2} v_p(a_3)\mathrm{e}\left(\frac{a_3(n+3d)^3}{p}\right)\right) + O(p)$$

$$= \frac{1}{16}p^2 + \frac{1}{16p}\sum_{j=0}^{3}\sum_{d\le p-1}\sum_{n\le p}\sum_{|a_j|<p/2} v_p(a_j)\mathrm{e}\left(\frac{a_j(n+jd)^3}{p}\right)$$

$$+ \frac{1}{16p^2}\sum_{0\le j<k\le 3}\sum_{d\le p-1}\sum_{n\le p}\sum_{|a_j|<p/2}\sum_{|a_k|<p/2} v_p(a_j)v_p(a_k)$$

$$\times\,\mathrm{e}\left(\frac{a_j(n+jd)^3+a_k(n+kd)^3}{p}\right)$$

$$+\frac{1}{16p^3}\sum_{0\le j<k<l\le 3}\sum_{d\le p-1}\sum_{n\le p}\sum_{|a_j|<p/2}\sum_{|a_k|<p/2}\sum_{|a_l|<p/2} v_p(a_j)v_p(a_k)v_p(a_l)$$
$$\times \mathrm{e}\left(\frac{a_j(n+jd)^3+a_k(n+kd)^3+a_l(n+ld)^3}{p}\right)$$
$$+\frac{1}{16p^4}\sum_{d\le p-1}\sum_{n\le p}\sum_{|a_0|<p/2}\sum_{|a_1|<p/2}\sum_{|a_2|<p/2}\sum_{|a_3|<p/2} v_p(a_0)v_p(a_1)v_p(a_2)v_p(a_3)$$
$$\times \mathrm{e}\left(\frac{a_0n^3+a_1(n+d)^3+a_2(n+2d)^3+a_3(n+3d)^3}{p}\right)$$
$$;=\frac{1}{16}p^2+\Omega_1+\Omega_2+\Omega_3+\Omega_4+O(p).$$

By Lemma 2.1 and Lemma 2.3 we easily get

$$\Omega_1=\frac{1}{16p}\sum_{j=0}^{3}\sum_{d\le p-1}\sum_{n\le p}\sum_{|a_j|<p/2} v_p(a_j)\mathrm{e}\left(\frac{a_j(n+jd)^3}{p}\right)$$
$$\ll \frac{1}{p}\sum_{j=0}^{3}\sum_{d\le p-1}\left(\sum_{\substack{|a_j|<p/2\\ a_j\neq 0}}\frac{p}{|a_j|}\right)\cdot p^{1/2}\ll p^{3/2}\log p.$$

From Lemma 2.4, Lemma 2.5 and Lemma 2.6 we also have

$$\Omega_2\ll p^{3/2}(\log p)^2,\quad \Omega_3\ll p^{3/2}(\log p)^3,\quad \Omega_4\ll p^{3/2}(\log p)^4.$$

Therefore

$$\sum_{d\le p}\sum_{n\le p}A_1(n)A_1(n+d)A_1(n+2d)A_1(n+3d)$$
$$=\frac{1}{16}p^2+O\left(p^{3/2}(\log p)^4\right)=\delta^4p^2+O\left(p^{3/2}(\log p)^4\right).$$

This proves Theorem 1.3.

Now we prove Theorem 1.4. By Lemma 2.1 we get

$$A_2(n)=\frac{1}{2p}\sum_{|a|<p/2}v_p(a)\mathrm{e}\left(\frac{an^2}{p}\right)+\frac{1}{2}. \tag{5.2}$$

Then from Lemma 2.1 and Lemma 2.3 we get

$$|A_2|=\sum_{n=1}^{p}A_2(n)=\frac{1}{2p}\sum_{|a|<p/2}v_p(a)\sum_{n=1}^{p}\mathrm{e}\left(\frac{an^2}{p}\right)+\frac{p}{2}$$

$$= \frac{p}{2} + O\left(\frac{1}{p} \sum_{\substack{|a|<p/2 \\ a\neq 0}} \frac{p}{|a|} \cdot p^{1/2} + 1\right) = \frac{p}{2} + O\left(p^{1/2} \log p\right).$$

Define $|A_2| = \delta p$, then $\delta = \frac{1}{2} + O\big(\frac{1}{p^{1/2} \log p}\big)$.

For $r \neq 0$, by Lemma 2.1 and Lemma 2.3 we get

$$\begin{aligned}
\hat{A}_2(r) &= \sum_{n=1}^{p} A_2(n) \mathrm{e}\left(-\frac{rn}{p}\right) \\
&= \frac{1}{2p} \sum_{|a|<p/2} v_p(a) \sum_{n=1}^{p} \mathrm{e}\left(\frac{an^2 - rn}{p}\right) + \frac{1}{2} \sum_{n=1}^{p} \mathrm{e}\left(-\frac{rn}{p}\right) \\
&\ll \frac{1}{p} \sum_{\substack{|a|<p/2 \\ a\neq 0}} \frac{p}{|a|} \cdot p^{1/2} \ll p^{1/2} \log p.
\end{aligned}$$

Then A_2 is uniform according to Definition 1.1. For any $k \neq 0$ and $r = R_p(2k)$, by Lemma 2.1 and Lemma 2.3 we get

$$\begin{aligned}
\widehat{\Delta(A_2; k)}(r) &= \sum_{n=1}^{p} A_2(n) A_2(n-k) \mathrm{e}\left(-\frac{rn}{p}\right) \\
&= \sum_{n=1}^{p} \left(\frac{1}{2p} \sum_{|a|<p/2} v_p(a) \mathrm{e}\left(\frac{an^2}{p}\right) + \frac{1}{2}\right) \\
&\quad \times \left(\frac{1}{2p} \sum_{|b|<p/2} v_p(b) \mathrm{e}\left(\frac{b(n-k)^2}{p}\right) + \frac{1}{2}\right) \mathrm{e}\left(-\frac{rn}{p}\right) \\
&= \frac{1}{4p^2} \sum_{|a|<p/2} v_p(a) \sum_{|b|<p/2} v_p(b) \sum_{n=1}^{p} \mathrm{e}\left(\frac{an^2 + b(n-k)^2 - rn}{p}\right) \\
&\quad + \frac{1}{4p} \sum_{|a|<p/2} v_p(a) \sum_{n=1}^{p} \mathrm{e}\left(\frac{an^2 - rn}{p}\right) \\
&\quad + \frac{1}{4p} \sum_{|b|<p/2} v_p(b) \sum_{n=1}^{p} \mathrm{e}\left(\frac{b(n-k)^2 - rn}{p}\right) + \frac{1}{4} \sum_{n=1}^{p} \mathrm{e}\left(-\frac{rn}{p}\right) \\
&= \frac{1}{4p^2} \sum_{|a|<p/2} v_p(a) \sum_{|b|<p/2} v_p(b) \sum_{n=1}^{p} \mathrm{e}\left(\frac{an^2 + b(n-k)^2 - rn}{p}\right) \\
&\quad + O\left(\frac{1}{p} \sum_{\substack{|a|<p/2 \\ a\neq 0}} \frac{p}{|a|} \cdot p^{1/2}\right)
\end{aligned}$$

$$= \frac{1}{4p^2} \sum_{\substack{|a|<p/2 \\ p|a+b}} \sum_{|b|<p/2} v_p(a)v_p(b) \sum_{n=1}^{p} \mathrm{e}\left(\frac{an^2 + b(n-k)^2 - rn}{p}\right)$$

$$+ O\left(\frac{1}{p^2} \sum_{\substack{|a|<p/2 \\ p\nmid a+b}} \sum_{|b|<p/2} |v_p(a)||v_p(b)| \cdot p^{1/2}\right) + O\left(p^{1/2}\log p\right)$$

$$= \frac{1}{4p^2} \sum_{|a|<p/2} v_p(a)v_p(-a) \sum_{n=1}^{p} \mathrm{e}\left(\frac{(2ka-r)n - ak^2}{p}\right) + O\left(p^{1/2}(\log p)^2\right)$$

$$= \frac{1}{4p} v_p(1)v_p(-1)\mathrm{e}\left(-\frac{k^2}{p}\right) \gg p.$$

Then A_2 is not quadratically uniform according to Definition 1.1.

On the other hand, from (5.2) we have

$$\sum_{d\le p} \sum_{n\le p} A_2(n)A_2(n+d)A_2(n+2d)A_2(n+3d)$$

$$= \sum_{d\le p-1} \sum_{n\le p} A_2(n)A_2(n+d)A_2(n+2d)A_2(n+3d) + O(p)$$

$$= \sum_{d\le p-1} \sum_{n\le p} \left(\frac{1}{2} + \frac{1}{2p} \sum_{|a_0|<p/2} v_p(a_0)\mathrm{e}\left(\frac{a_0 n^2}{p}\right)\right)$$

$$\times \left(\frac{1}{2} + \frac{1}{2p} \sum_{|a_1|<p/2} v_p(a_1)\mathrm{e}\left(\frac{a_1(n+d)^2}{p}\right)\right)$$

$$\times \left(\frac{1}{2} + \frac{1}{2p} \sum_{|a_2|<p/2} v_p(a_2)\mathrm{e}\left(\frac{a_2(n+2d)^2}{p}\right)\right)$$

$$\times \left(\frac{1}{2} + \frac{1}{2p} \sum_{|a_3|<p/2} v_p(a_3)\mathrm{e}\left(\frac{a_3(n+3d)^2}{p}\right)\right) + O(p)$$

$$= \frac{1}{16}p^2 + \frac{1}{16p} \sum_{j=0}^{3} \sum_{d\le p-1} \sum_{n\le p} \sum_{|a_j|<p/2} v_p(a_j)\mathrm{e}\left(\frac{a_j(n+jd)^2}{p}\right)$$

$$+ \frac{1}{16p^2} \sum_{0\le j<k\le 3} \sum_{d\le p-1} \sum_{n\le p} \sum_{|a_j|<p/2} \sum_{|a_k|<p/2} v_p(a_j)v_p(a_k)$$

$$\times \mathrm{e}\left(\frac{a_j(n+jd)^2 + a_k(n+kd)^2}{p}\right)$$

$$+\frac{1}{16p^3}\sum_{0\le j<k<l\le 3}\sum_{d\le p-1}\sum_{n\le p}\sum_{|a_j|<p/2}\sum_{|a_k|<p/2}\sum_{|a_l|<p/2} v_p(a_j)v_p(a_k)v_p(a_l)$$
$$\times \mathrm{e}\left(\frac{a_j(n+jd)^2+a_k(n+kd)^2+a_l(n+ld)^2}{p}\right)$$
$$+\frac{1}{16p^4}\sum_{d\le p-1}\sum_{n\le p}\sum_{|a_0|<p/2}\sum_{|a_1|<p/2}\sum_{|a_2|<p/2}\sum_{|a_3|<p/2} v_p(a_0)v_p(a_1)v_p(a_2)v_p(a_3)$$
$$\times \mathrm{e}\left(\frac{a_0n^2+a_1(n+d)^2+a_2(n+2d)^2+a_3(n+3d)^2}{p}\right)$$
$$;=\frac{1}{16}p^2+\Upsilon_1+\Upsilon_2+\Upsilon_3+\Upsilon_4+O(p).$$

By Lemma 2.1 and Lemma 2.3 we easily get

$$\Upsilon_1=\frac{1}{16p}\sum_{j=0}^{3}\sum_{d\le p-1}\sum_{n\le p}\sum_{|a_j|<p/2} v_p(a_j)\mathrm{e}\left(\frac{a_j(n+jd)^2}{p}\right)$$
$$\ll \frac{1}{p}\sum_{j=0}^{3}\sum_{d\le p-1}\left(\sum_{\substack{|a_j|<p/2\\ a_j\neq 0}}\frac{p}{|a_j|}\right)\cdot p^{1/2}\ll p^{3/2}\log p.$$

From Lemma 2.7, Lemma 2.8 and Lemma 2.9 we also have

$$\Upsilon_2\ll p^{3/2}(\log p)^2,\quad \Upsilon_3\ll p^{3/2}(\log p)^3,\quad \Upsilon_4=\frac{1}{8192}p^2+O\left(p^{3/2}(\log p)^4\right).$$

Therefore

$$\sum_{d\le p}\sum_{n\le p}A_2(n)A_2(n+d)A_2(n+2d)A_2(n+3d)$$
$$=\left(\frac{1}{16}+\frac{1}{8192}\right)p^2+O\left(p^{3/2}(\log p)^4\right)=\left(\delta^4+\frac{1}{8192}\right)p^2+O\left(p^{3/2}(\log p)^4\right).$$

This proves Theorem 1.4.

References

[1] J. Cassaigne, S. Ferenczi, C. Mauduit, J. Rivat and A. Sárközy, On finite pseudorandom binary sequencs III: the Liouville function, I, *Acta Arith.* **87** (1999), 367–390.

[2] H. Furstenberg, Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions, *J. Analyse Math.* **31** (1977), 204–256.

[3] H. Furstenberg, Y. Katznelson and D. Ornstein, The ergodic theoretical proof of Szemerédi's theorem, *Bull. Amer. Math. Soc. New Series* **7** (1982), 527–552.

[4] L. Goubin, C. Mauduit and A. Sárközy, Construction of large families of pseudorandom binary sequences, *J. Number Theory* **106** (2004), 56–69.

[5] W. T. Gowers, A new proof of Szemerédi's theorem, *Geom. Funct. Anal.* **11** (2001), 465–588.

[6] K. Gyarmati, On a family of pseudorandom binary sequences, *Period. Math. Hungar.* **49** (2004), 45–63.

[7] P. Hubert, C. Mauduit and A. Sárközy, On pseudorandom binary lattices, *Acta Arith.* **125** (2006), 51–62.

[8] C. Mauduit, J. Rivat and A. Sárközy, Construction of pseudorandom binary sequences using additive characters, *Monatsh. Math.* **141** (2004), 197–208.

[9] C. Mauduit and A. Sárközy, On finite pseudorandom binary sequences I: measure of pseudorandomness, the Legendre symbol, *Acta Arith.* **82** (1997), 365–377.

[10] C. Mauduit and A. Sárközy, Construction of pseudorandom binary sequences by using the multiplicative inverse, *Acta Math. Hungar.* **108** (2005), 239–252.

[11] C. Mauduit and A. Sárközy, On large families of pseudorandom binary lattices, *Unif. Distrib. Theory* **2** (2007), 23–37.

[12] H. Liu, New pseudorandom sequences constructed by quadratic residues and Lehmer numbers, *Proc. Amer. Math. Soc.* **135** (2007), 1309–1318.

[13] H. Liu, A family of pseudorandom binary sequences constructed by the multiplicative inverse, *Acta Arith.* **130** (2007), 167–180.

[14] K. F. Roth, On certain sets of integers, *J. London Math. Soc.* **28** (1953), 245–252.

[15] W. Schmidt, Equations Over Finite Fields: An Elementary Approach, Lecture Notes in Mathematics, *Springer*, *Berlin*, vol. 536, 1976.

[16] E. Szemerédi, On sets of integers containing no four elements in arithmetic progression, *Acta Math. Acad. Sci. Hungar.* **20** (1969), 89–104.

[17] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, *Acta Arith.* **27** (1975), 199–245.

[18] A. Weil, Sur les courbes algébriques et les variétés qui s'en déduisent, *Hermann*, *Paris*, 1948.

HUANING LIU
DEPARTMENT OF MATHEMATICS
NORTHWEST UNIVERSITY
XI'AN, SHAANXI
P.R. CHINA

E-mail: hnliumath@hotmail.com

XIAOYUN WANG
SCHOOL OF MATHEMATICS
SHANDONG UNIVERSITY
JINAN, SHANDONG
P.R. CHINA

E-mail: xywang@sdu.edu.cn

(Received September 2, 2010)