NEW PSEUDORANDOM SEQUENCES CONSTRUCTED
BY QUADRATIC RESIDUES AND LEHMER NUMBERS

HUANING LIU

(Communicated by Wen-Ching Winnie Li)

ABSTRACT. Let \( p \) be an odd prime. Define
\[
e_n = \begin{cases} 
(-1)^{n+\pi}, & \text{if } n \text{ is a quadratic residue mod } p, \\
(-1)^{n+\pi+1}, & \text{if } n \text{ is a quadratic nonresidue mod } p,
\end{cases}
\]
where \( \pi \) is the multiplicative inverse of \( n \) modulo \( p \) such that \( 1 \leq \pi \leq p - 1 \).

This paper shows that the sequence \( \{e_n\} \) is a “good” pseudorandom sequence,
by using the properties of exponential sums, character sums, Kloosterman
sums and mean value theorems of Dirichlet \( L \)-functions.

1. Introduction

Let \( p \) be an odd prime. For any integer \( n \) with \( 1 \leq n \leq p - 1 \), we define \( \pi \) to be
the multiplicative inverse of \( n \) modulo \( p \) such that \( 1 \leq \pi \leq p - 1 \). D. H. Lehmer \cite{7}
asked us to study the case that \( n \) and \( \pi \) are of opposite parity. In \cite{13} and \cite{14}
W. Zhang proved that
\[
\sum_{n=1}^{p-1} (-1)^{n+\pi} < p^{1/2} \log^2 p.
\]
Later he (partly with coauthors) gave a few generalizations on this subject (see
\cite{15}–\cite{18} for details). Recently S. R. Louboutin, J. Rivat and A. Sárközy \cite{8}
showed that the sequence \( \{(-1)^{n+\pi}\} \) forms a “good” pseudorandom sequence.

In a series of papers Mauduit, Rivat and Sárközy (partly with other coauthors)
studied finite pseudorandom binary sequences
\[
E_N = \{e_1, \cdots, e_N\} \in \{-1, +1\}^N.
\]
In \cite{9} Mauduit and 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 $a, b, t \in \mathcal{N}$ with $1 \leq a \leq a + (t - 1)b \leq N$. The correlation measure of order $k$ of $E_N$ is denoted as

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

where the maximum is taken over all $D = (d_1, \ldots, d_k)$ and $M$ with $0 \leq d_1 < \cdots < d_k \leq N - M$, 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 $a, b, t, D = (d_1, \ldots, d_k)$ with $1 \leq a + jb + d_i \leq N$ ($i = 1, 2, \cdots, k$).

In [10] the connection between the measures $W$ and $C_2$ was studied.

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 Cassaigne, Mauduit and Sárközy [4] proved that this terminology is justified since for almost all $E_N \in \{-1,+1\}^N$, both $W (E_N)$ and $C_k (E_N)$ are less than $N^{\frac{1}{2}} (\log N)^C$. Moreover, it was shown in [9] that the Legendre symbol forms a “good” pseudorandom sequence. In [2] and [3], Cassaigne and coauthors studied the pseudorandomness of the Liouville function, defined as $\lambda(n) = (-1)^{\Omega(n)}$ ($\Omega(n)$: number of prime factors of $n$ counted with multiplicity) and also of $\gamma(n) = (-1)^{\omega(n)}$ ($\omega(n)$: number of distinct prime factors of $n$). Furthermore, let

$$K(m,n;p) = \sum_{a=1}^{p-1} e\left(\frac{ma+n\pi}{p}\right)$$

denote the Kloosterman sum, where $e(y) = e^{2\pi i y}$, and $p$ is a prime. Fouvry (with other coauthors) [3] showed that the signs of $K(1,n;p)$ form a “good” pseudorandom binary sequence.

As was said in [9], the search for new approaches and new constructions should be continued. The purpose of this paper is to give some new examples of pseudorandom sequences. Let

$$e_n = \begin{cases} (-1)^{n+\chi_2}, & \text{if } n \text{ is a quadratic residue mod } p, \\ (-1)^{n+\chi_2+1}, & \text{if } n \text{ is a quadratic nonresidue mod } p, \end{cases}$$

(1.1)

where $\chi_2$ is the Legendre symbol. We shall prove that the sequence $\{e_n\}$ is a “good” pseudorandom sequence, that is, the following:

**Theorem 1.1.** Let $p$ be an odd prime, and let $E_{p-1} = \{e_1, \ldots, e_{p-1}\}$ be defined by (1.1). Then we have

$$W (E_{p-1}) \ll p^{\frac{2}{3}} \log^2 p;$$

$$C_2 (E_{p-1}) \ll p^{\frac{2}{3}} \log^3 p;$$

$$Q_2 (E_{p-1}) \ll p^{\frac{2}{3}} \log^3 p.$$
2. SOME LEMMAS

We need the following lemmas.

**Lemma 2.1.** Let \( p \) be a prime and let \( \chi \) be a Dirichlet character modulo \( p \). Define the generalized Kloosterman sum \( K(m, n; \chi; p) \) by

\[
K(m, n; \chi; p) = \sum_{a=1}^{p-1} \chi(a) e\left(\frac{ma + na}{p}\right).
\]

If \((m, n, p) = 1\), then we have

\[
|K(m, n; \chi; p)| \leq 2p^{\frac{1}{2}}.
\]

**Proof.** See reference [11]. \(\square\)

**Lemma 2.2.** Let \( p \) be a prime, let \( \chi \) be a Dirichlet character modulo \( p \), and let \( m \) and \( n \) be integers with \((n, p) = 1\). Then we have

\[
\sum_{a=1}^{p-1} (-1)^a \chi(a) e\left(\frac{ma + na}{p}\right) \ll \sqrt{p} \log p.
\]

**Proof.** From the trigonometric identity

\[
\sum_{u=1}^{p} e\left(\frac{un}{p}\right) = \begin{cases} p, & \text{if } p \mid n, \\ 0, & \text{if } p \nmid n, \end{cases}
\]

we have

\[
\sum_{a=1}^{p-1} (-1)^a \chi(a) e\left(\frac{ma + na}{p}\right) = \frac{1}{p} \sum_{a=1}^{p-1} \sum_{b=1}^{p} e\left(\frac{u(a - b)}{p}\right) (-1)^b \chi(a) e\left(\frac{ma + na}{p}\right)
\]

\[
= \frac{1}{p} \sum_{a=1}^{p-1} \sum_{b=1}^{p-1} (-1)^b e\left(-\frac{ub}{p}\right) \sum_{a=1}^{p-1} \chi(a) e\left(\frac{(m + u)a + na}{p}\right).
\]

Noting that

\[
\sum_{b=1}^{p-1} (-1)^b e\left(-\frac{ub}{p}\right) \ll \frac{1}{\sin\left(\frac{\pi}{p}\right)},
\]

then by Lemma 2.1 we get

\[
\sum_{a=1}^{p-1} (-1)^a \chi(a) e\left(\frac{ma + na}{p}\right) \ll \frac{1}{\sqrt{p}} \sum_{u=1}^{p} \frac{1}{\sin\left(\frac{\pi}{p}\right)} \ll \sqrt{p} \log p.
\]

This proves Lemma 2.2. \(\square\)
Lemma 2.3. Let \( \Psi \) be a nontrivial additive character, let \( \chi \) be a multiplicative character on a finite field \( \mathcal{F}_q \) of characteristic \( p \), let \( f, g \) be rational functions in \( \mathcal{F}_q(x) \) and let
\[
K(\Psi, f; \chi, g) = \sum_{x \in \mathcal{F}_q \setminus \mathfrak{s}} \chi(g(x))\Psi(f(x)),
\]
where \( \mathfrak{s} \) denotes the set of poles of \( f \) and \( g \). For \( f = f_1/f_2 \) we define \( \deg(f) = \deg(f_1) - \deg(f_2) \). If \( K(\Psi, f; \chi, g) \) is a nondegenerate sum with polynomial \( f \) and rational \( g \), we have
\[
|K(\Psi, f; \chi, g)| \leq (\deg(f) + l - 1) q^\frac{1}{2},
\]
where \( l \) is the number of distinct zeros and (non-infinite) poles of \( g \) in \( \overline{\mathcal{F}}_p \).

Proof. See reference [12].

Lemma 2.4. Let \( p \) be an odd prime, let \( \chi_2 \) be the Legendre symbol, and let \( \mathfrak{s} \) be integers with \( (rs, p) = 1 \). Then for \( 1 \leq a + tb + d_2 \leq p - 1, 0 \leq d_1 < d_2 \) and \( 1 \leq a + d_1 \), we have
\[
\Lambda = \sum_{j=0}^t \chi_2(a + jb + d_1)\chi_2(a + jb + d_2)e\left(\frac{ra + jb + d_1 + sa + jb + d_2}{p}\right) \ll p^\frac{1}{2} \log p.
\]

Proof. By (2.1) we get
\[
\begin{align*}
\Lambda &= \frac{1}{p} \sum_{j=0}^{p-1} \sum_{l=0}^t \sum_{u=0}^p e\left(\frac{u(j-l)}{p}\right) \chi_2(a + jb + d_1)\chi_2(a + jb + d_2) \\
&\quad \times e\left(\frac{ra + jb + d_1 + sa + jb + d_2}{p}\right) \\
&= \frac{1}{p} \sum_{u=1}^p \sum_{l=0}^t \sum_{j=0}^{p-1} e\left(-\frac{ul}{p}\right) \sum_{j=0}^{p-1} \chi_2(a + jb + d_1)\chi_2(a + jb + d_2) \\
&\quad \times e\left(\frac{ra + jb + d_1 + sa + jb + d_2 + uj}{p}\right).
\end{align*}
\]
Let \( g(j) = (a + jb + d_1)(a + jb + d_2) \) and
\[
f(j) = \frac{r(a + jb + d_2) + s(a + jb + d_1) + uj(a + jb + d_1)(a + jb + d_2)}{(a + jb + d_1)(a + jb + d_2)}.
\]
Then the sum
\[
\sum_{j=0}^{p-1} \chi_2(a + jb + d_1)\chi_2(a + jb + d_2)e\left(\frac{ra + jb + d_1 + sa + jb + d_2 + uj}{p}\right)
\]
\[
= \sum_{j=0}^{p-1} \chi_2(g(x))e\left(\frac{f(x)}{p}\right)
\]
is nondegenerate since \((rs, p) = 1\) and \(d_1 \neq d_2\). Noting that

\[
\sum_{l=0}^{t} e\left(-\frac{ul}{p}\right) \ll \frac{1}{\left|\sin\left(\frac{2u}{p}\right)\right|}, \quad \text{for } p \nmid u,
\]

then from Lemma 2.3 we have

\[
\Lambda \ll \frac{t}{\sqrt{p}} + \frac{1}{\sqrt{p}} \sum_{u=1}^{p-1} \frac{1}{\left|\sin\left(\frac{2u}{p}\right)\right|} \ll p^2 \log p.
\]

This completes the proof of Lemma 2.4. \(\square\)

**Lemma 2.5.** Let \(p\) be an odd prime and let \(k_1\) and \(k_2\) be nonnegative integers. Then for \(1 \leq a + tb + d_2 \leq p - 1, 0 \leq d_1 < d_2\) and \(1 \leq a + d_1\), we have

\[
\Upsilon = \sum_{j=0}^{t} \chi_2(a + jb + d_1) \chi_2(a + jb + d_2) \sum_{\chi'(-1) = -1, \chi''(-1) = -1} \sum_{\chi' \mod p} \sum_{\chi'' \mod p} \chi'(2^{k_1}) \chi''(2^{k_2})
\]

\[
\times \chi'(a + jb + d_1) \chi''(a + jb + d_2) \tau(\chi') \tau(\chi'') L(1, \chi') L(1, \chi'')
\]

\[
\ll p^{\frac{5}{2}} \log^3 p,
\]

where \(\chi_2\) is the Legendre symbol, \(\tau(\chi) = \sum_{a=1}^{p-1} \chi(a) e\left(\frac{a}{p}\right)\) is the Gauss sum, and \(L(1, \chi)\) denotes the Dirichlet L-function.

**Proof.** For any nonprincipal character \(\chi\) modulo \(p\), and parameter \(N \geq p\), by Abel’s identity we get

\[
L(1, \chi) = \sum_{n=1}^{+\infty} \chi(n) \frac{1}{n} = \sum_{1 \leq n \leq N} \chi(n) \frac{1}{n} + \int_{N}^{+\infty} \frac{\chi(n)}{y^2} dy
\]

\[
= \sum_{1 \leq n \leq N} \chi(n) \frac{1}{n} + O\left(\frac{\sqrt{p \log p}}{N}\right).
\]
Then we have
\[
\Upsilon = \sum_{j=0}^{t} \chi_2(a + jb + d_1) \chi_2(a + jb + d_2) \sum_{\chi' \left(\frac{-1}{-1} \equiv \chi'' \right), \chi' \equiv \chi'' \pmod{p}} \sum_{r=1}^{p-1} \chi'(r) e \left( \frac{r}{p} \right) \sum_{s=1}^{p-1} \chi''(s) e \left( \frac{s}{p} \right)
\]
\[
\times \sum_{1 \leq n \leq N} \sum_{1 \leq m \leq N} \frac{\Upsilon(n)}{n} \frac{\Upsilon'(m)}{m} + O \left( \frac{t \pi^2 \log p \log N}{N} \right)
\]
\[
= \sum_{j=0}^{t} \chi_2(a + jb + d_1) \chi_2(a + jb + d_2) \sum_{1 \leq u \leq N} \frac{1}{n} \sum_{1 \leq m \leq N} \frac{1}{m} \sum_{r=1}^{p-1} \chi'(r) e \left( \frac{r}{p} \right) \sum_{s=1}^{p-1} \chi''(s) e \left( \frac{s}{p} \right)
\]
\[
\times \sum_{\chi' \left(\frac{-1}{-1} \equiv \chi'' \right), \chi' \equiv \chi'' \pmod{p}} \chi'(2^{k_1}) \chi'(a + jb + d_1) \chi'(r) \Upsilon(n)
\]
\[
\times \sum_{\chi'' \left(\frac{-1}{-1} \equiv \chi'' \right), \chi'' \equiv \chi'' \pmod{p}} \chi''(2^{k_2}) \chi''(a + jb + d_2) \chi''(s) \Upsilon'(m) + O \left( \frac{t \pi^2 \log p \log N}{N} \right)
\]
\[
= \Omega + O \left( \frac{t \pi^2 \log p \log N}{N} \right)
\]
(2.4)

For \((ab, p) = 1\), from the orthogonality relation for character sums,
\[
\sum_{\chi \equiv a \pmod{p}} \chi(a) \chi(b) = \begin{cases} p-1, & \text{if } a \equiv b \pmod{p}, \\ 0, & \text{otherwise,} \end{cases}
\]
we get
\[
\sum_{\chi(-1) \equiv \chi \pmod{p}} \chi(a) \chi(b) = \begin{cases} \frac{1}{2}(p-1), & \text{if } a \equiv b \pmod{p}, \\ -\frac{1}{2}(p-1), & \text{if } a \equiv -b \pmod{p}, \\ 0, & \text{otherwise.} \end{cases}
\]

Therefore
\[
\Omega = \frac{(p-1)^2}{4} \sum_{j=0}^{t} \chi_2(a + jb + d_1) \chi_2(a + jb + d_2) \sum_{1 \leq n \leq N} \frac{1}{n} \sum_{1 \leq m \leq N} \frac{1}{m}
\]
\[
\times \sum_{r=1}^{p-1} e \left( \frac{r}{p} \right) \sum_{s=1}^{p-1} e \left( \frac{s}{p} \right)
\]
\[
2^{k_1} (a + jb + d_1) \equiv n \pmod{p} \quad 2^{k_2} (a + jb + d_2) \equiv m \pmod{p}
\]
\[
\sum_{r=1}^{p-1} e \left( \frac{r}{p} \right) \sum_{s=1}^{p-1} e \left( \frac{s}{p} \right)
\]
(2.6)
Similarly we get
\[
- \frac{(p-1)^2}{4} \sum_{j=0}^{t} \chi_2(a + jb + d_1) \chi_2(a + jb + d_2) \sum_{1 \leq n \leq N \atop (n,p) = 1} \frac{1}{n} \sum_{1 \leq m \leq N \atop (m,p) = 1} \frac{1}{m} \times \sum_{s=1}^{p-1} e \left( \frac{s}{p} \right) \sum_{r=1}^{p-1} e \left( \frac{r}{p} \right)
\]
\[
\times 2^{k_1(a+jb+d_1)r \equiv n \mod p} 2^{k_2(a+jb+d_2)s \equiv -m \mod p}
\]
\[
- \frac{(p-1)^2}{4} \sum_{j=0}^{t} \chi_2(a + jb + d_1) \chi_2(a + jb + d_2) \sum_{1 \leq n \leq N \atop (n,p) = 1} \frac{1}{n} \sum_{1 \leq m \leq N \atop (m,p) = 1} \frac{1}{m} \times \sum_{s=1}^{p-1} e \left( \frac{s}{p} \right) \sum_{r=1}^{p-1} e \left( \frac{r}{p} \right)
\]
\[
\times 2^{k_1(a+jb+d_1)r \equiv -n \mod p} 2^{k_2(a+jb+d_2)s \equiv -m \mod p}
\]
\[
+ \frac{(p-1)^2}{4} \sum_{j=0}^{t} \chi_2(a + jb + d_1) \chi_2(a + jb + d_2) \sum_{1 \leq n \leq N \atop (n,p) = 1} \frac{1}{n} \sum_{1 \leq m \leq N \atop (m,p) = 1} \frac{1}{m} \times \sum_{s=1}^{p-1} e \left( \frac{s}{p} \right) \sum_{r=1}^{p-1} e \left( \frac{r}{p} \right)
\]
\[
\times 2^{k_1(a+jb+d_1)r \equiv -n \mod p} 2^{k_2(a+jb+d_2)s \equiv -m \mod p}
\]
\[
= \Omega_1 + \Omega_2 + \Omega_3 + \Omega_4.
\]

By Lemma 2.4 we have
\[
\Omega_1 = \frac{(p-1)^2}{4} \sum_{1 \leq n \leq N \atop (n,p) = 1} \sum_{1 \leq m \leq N \atop (m,p) = 1} \frac{1}{n} \frac{1}{m} \sum_{j=0}^{t} \chi_2(a + jb + d_1) \chi_2(a + jb + d_2) \times e \left( \frac{n 2^{k_1(a+jb+d_1)} + m 2^{k_2(a+jb+d_2)}}{p} \right)
\]
\[
\leq p^{\frac{3}{2}} \log p \log^2 N.
\]

Similarly we get
\[
\Omega_2, \Omega_3, \Omega_4 \lesssim p^{\frac{3}{2}} \log p \log^2 N.
\]

Now taking $N = p^2$ in (2.4), (2.6), (2.7) and (2.8), we immediately have
\[
\Upsilon \ll p^{\frac{3}{2}} \log^3 p.
\]

This proves Lemma 2.5. \qed
3. Proof of the theorem

For \(a, b, t\) with \(1 \leq a \leq a + (t - 1)b \leq p - 1\), by (1.1) and (2.1) we have

\[
\sum_{j=0}^{t-1} e_{a+jb} = \sum_{j=0}^{t-1} (-1)^{a+jb+\overline{a+jb}} \chi_2(a+jb) \\
= \frac{1}{p^3} \sum_{j=0}^{p-1} \sum_{l=0}^{t-1} e\left(\frac{u(j-l)}{p}\right) \sum_{c=1}^{p-1} e\left(\frac{r(a+jb-c)}{p}\right) \\
\times \sum_{d=1}^{p-1} e\left(\frac{s(a+jb-d)}{p}\right) (-1)^{c+d} \chi_2(c) \\
= \frac{1}{p^3} \sum_{r=1}^{p} \sum_{s=1}^{p-1} \sum_{u=1}^{t-1} e\left(\frac{-ul}{p}\right) \sum_{c=1}^{p-1} (-1)^c \chi_2(c) e\left(\frac{-rc}{p}\right) \sum_{d=1}^{p-1} (-1)^d \left(\frac{-sd}{p}\right) \\
\times \sum_{j=0}^{p-1} e\left(\frac{r(a+jb+s\overline{a+jb}+uj)}{p}\right) \\
= \frac{1}{p^3} \sum_{r=1}^{p} \sum_{s=1}^{p-1} \sum_{u=1}^{t-1} e\left(\frac{-ul}{p}\right) \sum_{c=1}^{p-1} (-1)^c \chi_2(c) e\left(\frac{-rc}{p}\right) \sum_{d=1}^{p-1} (-1)^d \left(\frac{-sd}{p}\right) \\
\times e\left(\frac{-u\overline{a}\overline{b}}{p}\right) \sum_{t=1}^{p-1} e\left(\frac{rt+s\overline{t}+u\overline{b}t}{p}\right) \\
= \frac{1}{p} \sum_{s=1}^{p-1} \left(\sum_{d=1}^{p-1} (-1)^d e\left(\frac{-sd}{p}\right) \right) \sum_{u=1}^{t-1} e\left(\frac{-ul}{p}\right) e\left(\frac{-u\overline{a}\overline{b}}{p}\right) \\
\times \left(\sum_{t=1}^{p-1} (-1)^t \chi_2(t) e\left(\frac{u\overline{b}t+s\overline{t}}{p}\right) \right).
\]

Then by (2.2), (2.3) and Lemma 2.2 we get

\[
\sum_{j=0}^{t-1} e_{a+jb} \ll \frac{tp^2}{p^2} \sum_{s=1}^{p-1} \left|\frac{1}{\sin\left(\frac{\pi}{p}-\frac{\pi s}{p}\right)}\right| + \frac{tp^2}{p^2} \sum_{s=1}^{p-1} \left|\frac{1}{\sin\left(\frac{\pi}{p}-\frac{\pi u}{p}\right)}\right| \\
\ll p^{\frac{1}{2}} \log^2 p.
\]

Therefore

\[
W \left( E_{p-1} \right) = \max_{a,b,t} \left|\sum_{j=0}^{t-1} e_{a+jb}\right| \ll p^{\frac{1}{2}} \log^2 p.
\]
Therefore (3.1)

\[
\sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} = \sum_{j=0}^{t} (-1)^{a+jb+d_1+a+jb+d_2} \chi_2(a+jb+d_1)(-1)^{a+jb+d_2+\alpha+jb+d_2} \chi_2(a+jb+d_2)
\]

\[
= (-1)^{d_1+d_2} \sum_{j=0}^{t} (-1)^{a+jb+d_1+a+jb+d_2} \chi_2(a+jb+d_1) \chi_2(a+jb+d_2)
\]

\[
= \frac{(-1)^{d_1+d_2}}{(p-1)^2} \sum_{j=0}^{t} \sum_{p-1}^{p-1} \sum_{s=1}^{s=1} \chi'(r(a+jb+d_1)) \chi''(s(a+jb+d_2))
\]

\[
\times (-1)^{s} \chi_2(a+jb+d_1) \chi_2(a+jb+d_2)
\]

\[
= \frac{(-1)^{d_1+d_2}}{(p-1)^2} \sum_{j=0}^{t} \sum_{p-1}^{p-1} \sum_{p-1}^{p-1} (\chi'(a+jb+d_1) \chi_2(a+jb+d_1))
\]

\[
\times \chi''(a+jb+d_2) \chi_2(a+jb+d_2)
\]

\[
\times \sum_{r=1}^{p-1} (-1)^{r} \chi'(r) \sum_{s=1}^{s=1} (-1)^{s} \chi''(s).
\]

Noting that

\[
\sum_{r=1}^{p-1} (-1)^{r} \chi(r) = 0, \quad \text{if } \chi(-1) = 1,
\]

while if \( \chi(-1) = -1 \), from [6] and Theorem 12.11, 12.20 of [1] we have

\[
\sum_{r=1}^{p-1} (-1)^{r} \chi(r) = 2\chi(2) \sum_{r=1}^{(p-1)/2} \chi(r) = \frac{2(1-2\chi(2))}{p} \sum_{r=1}^{p-1} r\chi(r)
\]

\[
= \frac{2(1-2\chi(2))}{p} \tau(\chi)L(1, \chi).
\]

So from Lemma 2.5 we get

\[
\sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} = \frac{4(-1)^{d_1+d_2+1}}{\pi^2(p-1)^2} \sum_{j=0}^{t} \chi_2(a+jb+d_1) \chi_2(a+jb+d_2)
\]

\[
\times \sum_{\chi'(-1)=-1} \sum_{\chi''(-1)=-1} \chi'(a+jb+d_1) \chi''(a+jb+d_2)
\]

\[
\times \tau(\chi') \tau(\chi'') L(1, \chi') L(1, \chi'')
\]

\[
\ll p^{\frac{1}{4}} \log^3 p.
\]

Therefore

\[
(3.1) \quad Q_2(E_{p-1}) = \max_{a,b,t,D} \left| \sum_{j=0}^{t} e_{a+jb+d_1} e_{a+jb+d_2} \right| \ll p^{\frac{1}{4}} \log^3 p.
\]
Now taking $a = 0$, $b = 1$, $j = n - 1$ and $t = M - 1$ in (3.1), we immediately get
\[
C_2 (E_{p - 1}) = \max_{M,D} \left| \sum_{n=1}^{M} e_{n+d_1} e_{n+d_2} \right| \ll p^{\frac{1}{3}} \log^{3} p.
\]
This completes the proof of Theorem 1.1.

ACKNOWLEDGMENTS

The author expresses his gratitude to the referee for his detailed comments.

REFERENCES


DEPARTMENT OF MATHEMATICS, NORTHWEST UNIVERSITY, XI’AN, SHAANXI, PEOPLE’S REPUBLIC OF CHINA

E-mail address: hnl@nwu.edu.cn