Kloosterman-type sums
and the discrepancy of nonoverlapping pairs of inversive
congruential pseudorandom numbers

by

JÜRGEN EICHENAUER-HERRMANN (Darmstadt) and
HARALD NIEDERREITER (Wien)

1. Introduction and main results. In this paper a Kloosterman-
type exponential sum is discussed and applied to the analysis of certain
nonlinear congruential pseudorandom numbers. During the last few years
several nonlinear congruential methods of generating uniform pseudorandom
numbers in the interval $[0, 1)$ have been studied. A review of the development
of this area is given in the survey articles [2, 8, 9, 11] and in the monograph
[10]. One of these approaches is the inversive congruential method with
power of two modulus, which has been analysed in [1, 3, 4, 5, 7].

Let $m = 2^\omega$ for an integer $\omega \geq 6$. Let $Z_n = \{0, 1, \ldots, n-1\}$ for integers
$n \geq 2$ and write $Z_n^*$ for the set of all odd integers in $Z_n$. For integers $a, b \in Z_m$
with $a \equiv 1 \pmod{4}$ and $b \equiv 2 \pmod{4}$ an inversive congruential sequence
$(y_n)_{n \geq 0}$ of elements of $Z_m^*$ is defined by

$$y_{n+1} \equiv ay_n^{-1} + b \pmod{m}, \quad n \geq 0,$$

where $y_n^{-1}$ denotes the multiplicative inverse of $y_n$ modulo $m$. A sequence
$(x_n)_{n \geq 0}$ of inversive congruential pseudorandom numbers in the interval
$[0, 1)$ is obtained by $x_n = y_n / m$ for $n \geq 0$. It follows from [1] that these se-
quences are purely periodic with maximal period length $m/2$, i.e., $\{y_0, y_1, \ldots, y_{m/2-1}\} = Z_m^*$.

In the present paper the sequence $(x_n)_{n \geq 0}$ of nonoverlapping pairs of in-
nersive congruential pseudorandom numbers is considered, which is given by

$$x_n = (x_{2n}, x_{2n+1}), \quad n \geq 0,$$

and has period length $m/4$. In order to assess the uniformity of the distribution
of the points $x_0, x_1, \ldots, x_{m/4-1}$ in $[0, 1)^2$, their discrepancy $D_{m/4}^{(2)}$ is
studied, which is defined by
where the supremum is extended over all subrectangles $R$ of $[0, 1)^2$ with sides parallel to the axes, $F_{m/4}(R)$ is $4/m$ times the number of points among $x_0, x_1, \ldots, x_{m/4-1}$ falling into $R$, and $A(R)$ denotes the area of $R$. In the following main results upper and lower bounds for the discrepancy $D_{m/4}^{(2)}$ are established. Their proof is given in the third section. The method of proof relies on the detailed analysis of a Kloosterman-type sum in the second section.

**Theorem 1.** The discrepancy $D_{m/4}^{(2)}$ satisfies

$$D_{m/4}^{(2)} < \frac{4}{(2^{3/2} - 1)\pi^2} m^{-1/2} (\log m)^2 + (0.841)m^{-1/2} \log m + (1.274)m^{-1/2}$$

$$+ 4(\sqrt{2} + 1)m^{-1}$$

for any inversive congruential generator.

**Theorem 2.** The discrepancy $D_{m/4}^{(2)}$ satisfies

$$D_{m/4}^{(2)} \geq \frac{2^{3/2}}{B(\pi + 2)} m^{-1/2}$$

for any inversive congruential generator, where

$$B = \begin{cases} 1 & \text{for } a \equiv 1 \pmod{8}, \\ 3 & \text{for } a \equiv 5 \pmod{8}. \end{cases}$$

Theorem 1 shows that $D_{m/4}^{(2)} = O(m^{-1/2}(\log m)^2)$ for any inversive congruential sequence, where the implied constant is absolute. In particular, this bound is independent of the specific choice of the parameters $a, b,$ and $y_0$ in the inversive congruential method. Theorem 2 implies that the upper bound is best possible up to the logarithmic factor, since the discrepancy $D_{m/4}^{(2)}$ of any inversive congruential generator has an order of magnitude at least $m^{-1/2}$. It is in this range of magnitudes where one also finds the discrepancy of $m/4$ independent and uniformly distributed random points from $[0, 1)^2$, which should be of an order of magnitude $m^{-1/2}(\log\log m)^{1/2}$ according to the law of the iterated logarithm for discrepancies (cf. [6]). In this sense, inversive congruential pseudorandom numbers behave like true random numbers. Similar results have been obtained for the set of all (overlapping) pairs in the inversive congruential method (cf. [5,7]).

**2. Auxiliary results.** First, some further notation is necessary. For integers $k \geq 1$ and $q \geq 2$ let $C_k(q)$ be the set of all nonzero lattice points $(h_1, \ldots, h_k) \in \mathbb{Z}^k$ with $-q/2 < h_j \leq q/2$ for $1 \leq j \leq k$. Define
Kloosterman-type sums

\[ r(h, q) = \begin{cases} 
1 
& \text{for } h = 0, \\
q \sin \frac{\pi |h|}{q} 
& \text{for } h \in C_1(q),
\end{cases} \]

and

\[ r(h, q) = \prod_{j=1}^{k} r(h_j, q) \]

for \( h = (h_1, \ldots, h_k) \in C_k(q) \). For \( t \in \mathbb{R} \) the abbreviation \( e(t) = e^{2\pi it} \) is used, and \( \mathbf{u} \cdot \mathbf{v} \) stands for the standard inner product of \( \mathbf{u}, \mathbf{v} \in \mathbb{R}^k \).

Subsequently, three known results are stated. The first two lemmas are special versions of [10, Theorem 3.10 and Corollary 3.17] and the third lemma follows from [7, Lemma 4 and its proof].

**Lemma 1.** The discrepancy \( D_{m/4}^{(2)} \) satisfies

\[ D_{m/4}^{(2)} \leq \frac{2}{m} + \frac{4}{m} \sum_{h \in C_2(m)} r(h, m) \left| \sum_{n=0}^{m/4-1} e(h \cdot x_n) \right| . \]

**Lemma 2.** The discrepancy \( D_{m/4}^{(2)} \) satisfies

\[ D_{m/4}^{(2)} \geq \frac{2}{(\pi + 2)|h_1 h_2|m} \left| \sum_{n=0}^{m/4-1} e(h \cdot x_n) \right| \]

for any lattice point \( h = (h_1, h_2) \in \mathbb{Z}^2 \) with \( h_1 h_2 \neq 0 \).

**Lemma 3.** Let \( t \geq 6 \) be an integer and \( c \in \mathbb{Z}_8^* \). Then

\[ \sum_{\substack{k \in C_1(2^t) \\
k \equiv c \pmod{8}}} \frac{1}{r(k, 2^t)} < \frac{1}{4\pi} \log 2^t + \begin{cases} 
0.2676 & \text{for } c \in \{1, 7\}, \\
0.0341 & \text{for } c \in \{3, 5\}.
\end{cases} \]

Lemmas 1 and 2 show that the exponential sums \( \sum_{n=0}^{m/4-1} e(h \cdot x_n) \) are of interest in estimating the discrepancy \( D_{m/4}^{(2)} \). Since \( \{y_0, y_2, \ldots, y_{m/2-2}\} = \{y \in \mathbb{Z}_m \mid y \equiv y_0 \pmod{4}\} \), it follows at once that

\[ \left| \sum_{n=0}^{m/4-1} e(h \cdot x_n) \right| = \left| \sum_{n=0}^{m/4-1} e((h_1 y_{2n} + h_2 y_{2n+1})/m) \right| = \left| \sum_{n=0}^{m/4-1} e((h_1 y_{2n} + h_2 y_{2n+1})/m) \right| = \left| \sum_{y \in \mathbb{Z}_m} e((h_1 y + h_2 y^{-1})/m) \right|. \]
for $h = (h_1, h_2) \in \mathbb{Z}^2$. This motivates the following definition. For integers $u, v \in \mathbb{Z}$, $\xi \in \{1, 3\}$, and $\alpha \geq 2$ the Kloosterman-type sum

$$S(u, v, \xi; 2^\alpha) = \sum_{y \equiv \xi \pmod{4}} e((uy + vy^{-1})/2^\alpha)$$

is introduced. In order to evaluate these exponential sums in Lemma 5, the mapping

$$\Phi = (\phi_1, \phi_2): \mathbb{Z}^2 \to \mathbb{Z}^2 \quad \text{with} \quad \Phi(y, z) = (yz, y - z)$$

is studied in the subsequent lemma. For integers $\alpha \geq 3$ let

$$N_\alpha = \{(s, t) \in \mathbb{Z}_{2^\alpha}^2 \mid t \equiv 0 \pmod{4}, \ s \equiv t + 1 \pmod{8}\}.$$ Observe that $\Phi(y, z) \mod 2^\alpha \in N_\alpha$ for all $y, z \in \mathbb{Z}$ with $y \equiv z \equiv \xi \pmod{4}$.

**Lemma 4.** Let $(s, t) \in N_\alpha$ for some integer $\alpha \geq 3$. Then there exists exactly one $(y, z) \in \mathbb{Z}_{2^\alpha - 1} \times \mathbb{Z}_{2^\alpha}$ with $y \equiv z \equiv \xi \pmod{4}$ and

$$\Phi(y, z) \equiv (s, t) \mod 2^\alpha.$$ Proof. For integers $\alpha \geq 3$ and $(s, t) \in N_\alpha$ let

$$M_\alpha(s, t) = \{(y, z) \in \mathbb{Z}_{2^\alpha}^2 \mid y \equiv z \equiv \xi \pmod{4}, \ \Phi(y, z) \equiv (s, t) \mod 2^\alpha\}.$$ Subsequently, it is proved by induction on $\alpha \geq 3$ that for any $(s, t) \in N_\alpha$ the set $M_\alpha(s, t)$ contains exactly two elements, say $(y, z)$ and $(y', z')$, which satisfy $(y', z') \equiv (y + 2^\alpha - 1, z + 2^\alpha - 1) \pmod{2^\alpha}$. This statement is equivalent to the assertion of Lemma 4, since $\Phi(y + 2^\alpha - 1, z + 2^\alpha - 1) \equiv \Phi(y, z) \mod 2^\alpha$ for odd integers $y$ and $z$.

For $\alpha = 3$ the above statement can be shown by inspection, since $N_3 = \{(1, 0), (5, 4)\}$, $M_3(1, 0) = \{(\xi, \xi), (\xi + 4, \xi + 4)\}$, and $M_3(5, 4) = \{(\xi, \xi + 4), (\xi + 4, \xi)\}$. Now, assume that it is valid for some integer $\alpha \geq 3$. Let $(s, t) \in N_{\alpha + 1}$ be fixed. Then $(s, t) \mod 2^\alpha \in N_\alpha$, and the induction hypothesis implies that there exists an element $(y_\alpha, z_\alpha) \in \mathbb{Z}_{2^\alpha}^2$ with $y_\alpha \equiv z_\alpha \equiv \xi \pmod{4}$ and $\Phi(y_\alpha, z_\alpha) \equiv (s, t) \mod 2^\alpha$. Hence,

$$\Phi(y_\alpha, z_\alpha) \equiv (s, t) + 2^\alpha (\tilde{s}, \tilde{t}) \pmod{2^{\alpha + 1}}$$

with suitable $\tilde{s}, \tilde{t} \in \mathbb{Z}_2$. In the following let $(y, z) \in \mathbb{Z}_{2^{\alpha + 1}}^2$ be an arbitrary element. It suffices to consider the case $(y, z) \mod 2^\alpha \in M_\alpha(s, t)$, since otherwise $(y, z)$ cannot belong to the set $M_{\alpha + 1}(s, t)$. Therefore, by the induction hypothesis, $(y, z) \equiv (y_\alpha, z_\alpha) + 2^{\alpha - 1}(\lambda, \lambda) \pmod{2^\alpha}$ with a suitable $\lambda \in \mathbb{Z}_2$. Hence, one obtains

$$(y, z) \equiv (y_\alpha, z_\alpha) + 2^{\alpha - 1}(\lambda, \lambda) + 2^\alpha (\tilde{y}, \tilde{z}) \pmod{2^{\alpha + 1}}$$
with suitable \( \tilde{y}, \tilde{z} \in \mathbb{Z}_2 \). A short calculation shows that
\[
\Phi(y, z) \equiv \Phi(y_\alpha + 2^{\alpha - 1}\lambda + 2^{\alpha - 1}\tilde{y}, z_\alpha + 2^{\alpha - 1}\lambda + 2^{\alpha - 1}\tilde{z}) \\
\equiv \Phi(y_\alpha, z_\alpha) + 2^{\alpha}(\lambda + \tilde{y} + \tilde{z}, \tilde{y} + \tilde{z}) \\
\equiv (s, t) + 2^{\alpha}(\lambda + \tilde{y} + \tilde{z} + \tilde{s}, \tilde{y} + \tilde{z} + \tilde{t}) \pmod{2^{\alpha + 1}}.
\]
Therefore, an element \((y, z) \in \mathbb{Z}_{2^{\alpha + 1}}^2\) belongs to \(M_{\alpha + 1}(s, t)\) if and only if
\[
\lambda + \tilde{s} + \tilde{t} \equiv \tilde{y} + \tilde{t} \equiv 0 \pmod{2} \quad \text{and} \quad \lambda + \tilde{s} + \tilde{t} \equiv 0 \pmod{2}.
\]
Hence, \(\lambda + \tilde{s} + \tilde{t} \equiv 0 \pmod{2}\) with a suitable \(\tilde{\lambda} \in \mathbb{Z}_2\) and
\[
(y, z) \equiv (y_\alpha + 2^{\alpha - 1}(\tilde{s} + \tilde{t}), z_\alpha + 2^{\alpha - 1}(\tilde{s} - \tilde{t})) + 2^{\alpha}(\lambda', \lambda') \pmod{2^{\alpha + 1}},
\]
where \(\lambda' \equiv \tilde{\lambda} + \tilde{y} \pmod{2}\). Consequently, the set \(M_{\alpha + 1}(s, t)\) contains exactly two elements which stand in the desired relation. This completes the proof.

**Lemma 5.** Let \(u, v \in \mathbb{Z}\) and \(\xi \in \{1, 3\}\).

(a) If \(u + v \equiv 1 \pmod{2}\) and \(\alpha \geq 3\), then
\[
S(u, v, \xi; 2^\alpha) = 0.
\]
(b) If \(u \equiv v \equiv 0 \pmod{2}\) and \(\alpha \geq 3\), then
\[
S(u, v, \xi; 2^\alpha) = 2S(u/2, v/2, \xi; 2^{\alpha - 1}).
\]
(c) If \(u \equiv v \equiv 1 \pmod{2}\), then
\[
|S(u, v, \xi; 8)| = 2,
\]
\[
|S(u, v, \xi; 16)| = \begin{cases} 
4 & \text{for } u \equiv v \pmod{4}, \\
0 & \text{for } u \not\equiv v \pmod{4},
\end{cases}
\]
\[
|S(u, v, \xi; 32)| = \begin{cases} 
8 & \text{for } u \equiv 5v \pmod{8}, \\
0 & \text{for } u \not\equiv 5v \pmod{8},
\end{cases}
\]
and for \(\alpha \geq 6\)
\[
|S(u, v, \xi; 2^\alpha)| = \begin{cases} 
2^{(\alpha+1)/2} & \text{for } u \equiv v \pmod{8}, \\
0 & \text{for } u \not\equiv v \pmod{8}.
\end{cases}
\]

**Proof.** (a) A short calculation shows that
\[
S(u, v, \xi; 2^\alpha)
= \sum_{y \in \mathbb{Z}_{2^{\alpha + 1}} \atop y \equiv \xi \pmod{4}} (e((uy + vy^{-1})/2^\alpha) + e((u(y + 2^{\alpha - 1}) + v(y + 2^{\alpha - 1})^{-1})/2^\alpha))
= \sum_{y \in \mathbb{Z}_{2^{\alpha - 1}} \atop y \equiv \xi \pmod{4}} e((uy + vy^{-1})/2^\alpha)(1 + e((u + v)/2)).
\]
Therefore the desired result follows at once from $e((u + v)/2) = -1$ for $u + v \equiv 1 \pmod{2}$.

(b) Since $e((u + v)/2) = 1$ for $u + v \equiv 0 \pmod{2}$, it follows from part (a) of the proof that

$$S(u, v, \xi; 2^\alpha) = 2 \sum_{y \in \mathbb{Z}_{2^{\alpha-1}}, \ \ y \equiv \xi \pmod{4}} e((u/2)y + (v/2)y^{-1})/2^{\alpha-1})$$

$$= 2S(u/2, v/2, \xi; 2^{\alpha-1}).$$

(c) Subsequently, the cases $3 \leq \alpha \leq 5$ are considered. A straightforward calculation shows that $(4\eta + \xi)^{-1} \equiv 12\eta + \xi^{-1} \pmod{2^\alpha}$ for $\eta \in \mathbb{Z}$, and hence

$$|S(u, v, \xi; 2^\alpha)| = \left| \sum_{\eta \in \mathbb{Z}_{2^{\alpha-2}}} e((u(4\eta + \xi) + v(4\eta + \xi)^{-1})/2^\alpha) \right|$$

$$= \left| \sum_{\eta \in \mathbb{Z}_{2^{\alpha-2}}} e((u + 3v)\eta/2^{\alpha-2}) \right|$$

$$= \begin{cases} 2^{\alpha-2} & \text{for } u + 3v \equiv 0 \pmod{2^{\alpha-2}}, \\ 0 & \text{for } u + 3v \not\equiv 0 \pmod{2^{\alpha-2}}, \end{cases}$$

which yields the desired results. Now, the case $\alpha \geq 6$ is considered. First, one obtains

$$|S(u, v, \xi; 2^\alpha)|^2 = S(u, v, \xi; 2^\alpha)S(u, v, \xi; 2^\alpha)$$

$$= \sum_{y, z \in \mathbb{Z}_{2^\alpha}} e((u - v(y - z) + v(y^{-1} - z^{-1}))/2^\alpha)$$

$$= \sum_{y, z \in \mathbb{Z}_{2^\alpha}, \ \ y \equiv z \pmod{2^\alpha}} e((u - v(\phi_1(y, z))^{-1})\phi_2(y, z)/2^\alpha),$$

where the mapping $\Phi = (\phi_1, \phi_2)$ is defined as above. Since $\Phi(y + 2^{\alpha-1}, z + 2^{\alpha-1}) \equiv \Phi(y, z) \pmod{2^\alpha}$ for odd integers $y$ and $z$, it follows together with Lemma 4 that

$$|S(u, v, \xi; 2^\alpha)|^2 = 2 \sum_{(y, z) \in \mathbb{Z}_{2^{\alpha-1}} \times \mathbb{Z}_{2^\alpha}, \ \ y \equiv z \pmod{2^\alpha}} e((u - v(\phi_1(y, z))^{-1})\phi_2(y, z)/2^\alpha)$$

$$= 2 \sum_{(s, t) \in N_{\alpha}} e((u - vs^{-1})t/2^\alpha) = 2\left(\sum_1 + \sum_2\right),$$

where the abbreviations

$$\sum_1 = \sum_{s \in \mathbb{Z}_{2^\alpha}, \ \ s \equiv 1 \pmod{8}} \sum_{t \in \mathbb{Z}_{2^\alpha}, \ \ t \equiv 0 \pmod{8}} e((u - vs^{-1})t/2^\alpha)$$
and
\[ \sum_2 = \sum_{s \in \mathbb{Z}_{2^{\alpha}}} \sum_{t \in \mathbb{Z}_{2^{\alpha}}} e((u - vs^{-1})t/2^{\alpha}) \]
are used. Straightforward calculations show that

\[ \sum_1 = \sum_{s \in \mathbb{Z}_{2^{\alpha}}} \sum_{\tau \in \mathbb{Z}_{2^{\alpha} - 3}} e((u - vs^{-1})\tau/2^{\alpha - 3}) \]
\[ = 2^{\alpha - 3} \cdot \# \{ s \in \mathbb{Z}_{2^{\alpha}} \mid s \equiv 1 \pmod{8}, us \equiv v \pmod{2^{\alpha - 3}} \} \]
\[ = \begin{cases} 2^{\alpha} & \text{for } u \equiv v \pmod{8}, \\ 0 & \text{for } u \not\equiv v \pmod{8} \end{cases} \]

and

\[ \sum_2 = \sum_{s \in \mathbb{Z}_{2^{\alpha}}} \sum_{\tau \in \mathbb{Z}_{2^{\alpha} - 2}} e((u - vs^{-1})\tau/2^{\alpha - 2}) \]
\[ = 4 \sum_{s \in \mathbb{Z}_{2^{\alpha} - 3}} \sum_{\tau \in \mathbb{Z}_{2^{\alpha} - 2}} (e((u - vs^{-1})\tau/2^{\alpha - 2}) + e((u - v(s+2^{\alpha - 3}^{-1})\tau/2^{\alpha - 2})) \]
\[ = 4 \sum_{s \in \mathbb{Z}_{2^{\alpha} - 3}} \sum_{\tau \in \mathbb{Z}_{2^{\alpha} - 2}} e((u - vs^{-1})\tau/2^{\alpha - 2})(1 + e(v\tau/2)) = 0, \]

since \( e(v\tau/2) = -1 \) for any \( \tau \in \mathbb{Z}_{2^{\alpha} - 2} \). This completes the proof.

3. Proof of the main results

Proof of Theorem 1. First, Lemma 1 is applied, which yields
\[ D_{m/4}^{(2)} \leq \frac{2}{m} + \frac{4}{m} \sum_{h \in C_2(m)} \frac{1}{r(h, m)} |S(h_1, h_2a, \xi; m)|, \]
where \( \xi \equiv y_0 \pmod{4} \) is \( \in \{1, 3\} \). Now, Lemma 5 can be used in order to obtain
\[ D_{m/4}^{(2)} \leq \frac{2}{m} + \frac{4}{m} \sum_{h \in C_2(m)} \frac{1}{r(h, m)} |S(h_1, h_2a, \xi; m)| \]
\[ + \frac{4}{m} \sum_{\gamma = 0}^{2^{\alpha - 3}} \sum_{\gcd(h_1, h_2, m) = 2^{\gamma}} \frac{1}{r(h, m)} |S(h_1, h_2a, \xi; m)| \]
\[
\begin{align*}
&= \frac{2}{m} + \sum_{h \in C_2(m)} \frac{1}{r(h, m)} \\
&\quad + \frac{4}{m} \sum_{\gamma=0}^{\omega-3} 2^{\gamma} \sum_{h \in C_2(m)} \frac{1}{r(h, m)} |S(h_1/2^\gamma, h_2a/2^\gamma, \xi; 2^{\omega-\gamma})| \\
&\quad + \frac{4}{m} \sum_{\gamma=0}^{\omega-3} 2^{\gamma} \sum_{h \in C_2(m)} \frac{1}{r(h, m)} |S(h_1/2^\gamma, h_2a/2^\gamma, \xi; 2^{\omega-\gamma})| \\
&\quad = \frac{2}{m} + \left( \sum_{k \in C_1(4)} \frac{1}{r(2^{\omega-2}k, m)} + 1 \right)^2 - 1 \\
&\quad + \frac{4}{m} \sum_{\gamma=0}^{\omega-3} 2^{\gamma} \sum_{k \in C_2(2^{\omega-\gamma})} \frac{1}{r(2^\gamma k, m)} |S(k_1, k_2a, \xi; 2^{\omega-\gamma})| \\
&\quad = \frac{2}{m} + \left( \frac{1}{m} (2\sqrt{2} + 1) + 1 \right)^2 - 1 \\
&\quad + \frac{4}{m} \sum_{\gamma=0}^{\omega-3} 2^{\gamma} \sum_{k \in C_2(2^{\omega-\gamma})} \frac{1}{r(2^\gamma k, m)} |S(k_1, k_2a, \xi; 2^{\omega-\gamma})| \\
&\quad = \frac{4(\sqrt{2} + 1)}{m} + \frac{4\sqrt{2} + 9}{m} + \frac{64}{m^2} \sum_{k \in C_2(8)} \frac{1}{r(k, 8)} \\
&\quad + \frac{256}{m^2} \sum_{k \in C_2(16)} \frac{1}{r(k, 16)} + \frac{1024}{m^2} \sum_{k \in C_2(32)} \frac{1}{r(k, 32)} \\
&\quad + \frac{4}{m} \sum_{\gamma=0}^{\omega-6} 2^{-\gamma+(\omega-\gamma+1)/2} \sum_{k \in C_2(2^{\omega-\gamma})} \frac{1}{r(k, 2^{\omega-\gamma})} \\
&\quad = \frac{4(\sqrt{2} + 1)}{m} + \frac{4\sqrt{2} + 9}{m} \\
&\quad + \frac{64}{m^2} \left( \sum_{k \in C_1(8)} \frac{1}{r(k, 8)} \right)^2 + \frac{512}{m^2} \left( \sum_{k \in C_1(16)} \frac{1}{r(k, 16)} \right)^2
\end{align*}
\]
Hence, straightforward computations and an application of Lemma 3 show that

\[
D_{m/4}^{(2)} < 4(\sqrt{2} + 1) \frac{m}{m^2} + \frac{236.66}{m^2} + \frac{2048}{m^2} \sum_{d \in \{1,3\}} \left( \sum_{k \in C_1(32) \atop k \equiv 5ad \pmod{8}} \frac{1}{r(k,32)} \right)^2 \left( \sum_{k \in C_1(32) \atop k \equiv d \pmod{8}} \frac{1}{r(k,32)} \right)^2 \\
+ \frac{8\sqrt{2}}{m^{1/2}} \sum_{\gamma=0}^{\omega^{-6}} 2^{-3\gamma/2} \sum_{d \in \{1,3\}} \left( \sum_{k \in C_1(2^{\omega-\gamma}) \atop k \equiv d \pmod{8}} \frac{1}{r(k,2^{\omega-\gamma})} \right)^2 \left( \sum_{k \in C_1(2^{\omega-\gamma}) \atop k \equiv d \pmod{8}} \frac{1}{r(k,2^{\omega-\gamma})} \right)^2 \\
< 4(\sqrt{2} + 1) \frac{m}{m^2} + \frac{753}{m^2} \\
+ \frac{8\sqrt{2}}{m^{1/2}} \sum_{\gamma=0}^{\omega^{-5}} 2^{-3\gamma/2} \left( \frac{1}{8\pi^2} (\log 2^{\omega-\gamma})^2 + \frac{0.15085}{\pi} \log 2^{\omega-\gamma} + 0.072773 \right) \\
< 4(\sqrt{2} + 1) \frac{m}{m^2} \\
+ \frac{8\sqrt{2}}{m^{1/2}} \sum_{\gamma=0}^{\omega^{-5}} 2^{-3\gamma/2} \left( \frac{1}{8\pi^2} (\log 2^{\omega-\gamma})^2 + \frac{0.15085}{\pi} \log 2^{\omega-\gamma} + 0.072773 \right) \\
< 4(\sqrt{2} + 1) \frac{m}{m^2} \\
+ \frac{8\sqrt{2}}{m^{1/2}} \sum_{\gamma=0}^{\infty} 2^{-3\gamma/2} \left( \frac{1}{8\pi^2} (\log m)^2 + \frac{0.15085}{\pi} \log m + 0.072773 \right) \\
= 4(\sqrt{2} + 1) \frac{m}{m^2} \\
+ \frac{32}{(2^{3/2} - 1)m^{1/2}} \left( \frac{1}{8\pi^2} (\log m)^2 + \frac{0.15085}{\pi} \log m + 0.072773 \right). \quad \blacksquare
\]

Proof of Theorem 2. First, Lemma 2 is applied with \( \mathbf{h} = (B,-1)^{(B-1)/2} \in \mathbb{Z}^2 \), which yields
\[ D_{m/4}^{(2)} \geq \frac{2}{B(\pi + 2)m} |S(B, (-1)^{(B-1)/2}a, \xi; m)|, \]

where \( \xi \equiv y_0 \text{ (mod 4)} \in \{1, 3\} \). Since \( B \equiv (-1)^{(B-1)/2}a \text{ (mod 8)} \), it follows from Lemma 5(c) that

\[ |S(B, (-1)^{(B-1)/2}a, \xi; m)| = (2m)^{1/2}, \]

which completes the proof.  

References


