ACTA ARITHMETICA
136.2 (2009)

A note on the pseudorandomness of the Liouville function

by

HUANING LIU (Xi'an) and WENGUANG ZHAI (Jinan)

1. Introduction. For integer $n \geq 1$, the *Liouville function* $\lambda(n)$ is defined by

$$\lambda(n) = (-1)^{\alpha_1+\cdots+\alpha_k}, \quad \text{where} \quad n = p_1^{\alpha_1}\cdots p_k^{\alpha_k}.$$

It is natural to expect that the sequence $\{\lambda(n)\}$ behaves like a random sequence of $\pm$ signs. Recently J. Cassaigne and coauthors [2, 3] studied the pseudorandomness of the pseudorandom binary sequence constructed by the Liouville function.

In a series of papers C. Mauduit, J. Rivat and A. Sárközy (partly with other coauthors) studied finite pseudorandom binary sequences

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

In [17] C. Mauduit and A. Sárközy introduced the following measures of pseudorandomness: the *well-distribution measure* of E_N is defined by

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

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

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

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 by*

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

2000 *Mathematics Subject Classification*: 11K45, 11K38.
Key words and phrases: Liouville function, well-distribution, correlation, quasirandom.

DOI: 10.4064/aa136-2-1

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

The sequence is considered to be 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. J. Cassaigne, C. Mauduit and A. 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 $N^{1/2}(\log N)^c$. Moreover, [17] was followed by a series of papers in which numerous sequences were constructed and tested for pseudorandomness. Previous related results can be found in [9–12, 14–16, 18, 20].

Let $L_N = \{\lambda(1), \dots, \lambda(N)\}$. J. Cassaigne and coauthors [2] showed that the well-distribution measure of L_N is small. More precisely, they proved the following:

Proposition 1.1.

(I) *For any real number $A > 0$, for $N > N_0(A)$, we have*

$$W(L_N) < N(\log N)^{-A}.$$

(II) *Under the generalized Riemann hypothesis (GRH), for $\varepsilon > 0$ and $N > N_1(\varepsilon)$, we have*

$$W(L_N) < N^{5/6+\varepsilon}.$$

Since the Riemann hypothesis is equivalent to $\sum_{n \le x} \lambda(n) = O(x^{1/2+\varepsilon})$, it is very hard to prove $W(L_N) \ll N^{1/2+\varepsilon}$ unconditionally. However, the estimate of $W(L_N)$ can be improved under GRH. In Section 2 we shall prove the following theorem by using the classical methods in analytic number theory.

Theorem 1.1. *For sufficiently large N, we have*

$$W(L_N) \ll N^{1/2+\varepsilon} \quad \text{under GRH.}$$

Estimating the correlation measure of L_N is rather difficult. G. Harman, J. Pintz and D. Wolke [13] proved that

$$(1 + o(1))\,\frac{1}{3} < \frac{1}{x} \sum_{n \le x} \lambda(n)\lambda(n+1) < 1 - \frac{1}{(\log x)^{7+\varepsilon}}.$$

P. D. T. A. Elliott [8] showed that

$$\liminf_{x \to \infty} \frac{1}{x} \sum_{n \le x} \lambda(n)\lambda(n+1)\lambda(n+2) \le \frac{20}{21}.$$

J. Cassaigne and coauthors [2] proved that

$$\Big|\sum_{n\le x}\lambda(n)\lambda(n+d)\cdots\lambda(n+2kd)\Big| \le \begin{cases}\Big(1-\dfrac{2}{3(2k+1)}\Big)x+O(\log x) & \text{if } d \text{ is even},\\ \Big(1-\dfrac{2}{3(k+1)}\Big)x+O(\log x) & \text{if } d \text{ is odd}\end{cases}$$

and

$$\sum_{n\le x}\lambda(n)\lambda(n+d)\cdots\lambda(n+(2k-1)d) \ge \begin{cases}-\Big(1-\dfrac{2}{3k}\Big)x+O(\log x) & \text{if } d \text{ is odd},\\ -\Big(1-\dfrac{1}{3k}\Big)x+O(\log x) & \text{if } d \text{ is even}.\end{cases}$$

Let $\mathbb{Z}_N$ be the ring of integers modulo N. In Section 4 we shall prove some related results for the Liouville function, by using quasirandom subsets of $\mathbb{Z}_N$.

Theorem 1.2. *Define* $L'_{2N}=\{\lambda'(1),\ldots,\lambda'(2N)\}$, *where*

$$\lambda'(n)=\begin{cases}\lambda(n) & \text{if } 1\le n\le N,\\ \lambda(n-N) & \text{if } N+1\le n\le 2N.\end{cases}$$

Let $A>0$ *and* $k\ge 2$ *be any fixed integers, and define*

$$F_1(N)=\begin{cases}N(\log N)^{-A} & \text{unconditionally},\\ N^{7/8+\varepsilon} & \text{under GRH}.\end{cases}$$

(I) *For all except* $O(F_1(N))$ *elements* $u_1,\ldots,u_k$ *of* $\mathbb{Z}_N$, *we have*

$$\sum_{n=1}^{N}\lambda'(n+u_1)\cdots\lambda'(n+u_k)=O(F_1(N)).$$

(II) *For all except* $O(F_1(N))$ *elements* x *of* $\mathbb{Z}_N$, *we have*

$$\sum_{\substack{n_1=1\\ n_1+\cdots+n_k\equiv x\,(\mathrm{mod}\,N)}}^{N}\cdots\sum_{n_k=1}^{N}\lambda(n_1)\cdots\lambda(n_k)=O(N^{k-2}F_1(N)).$$

From Theorem 1.2(I) we immediately get the following corollary.

Corollary 1.1. *For all except* $O(F_1(N))$ *elements* $d_1,\ldots,d_k$ *of* $\mathbb{Z}_N$ *satisfying* $0\le d_1<\cdots<d_k=O(F_1(N))$, *we have*

$$\sum_{n\le N-d_k}\lambda(n+d_1)\cdots\lambda(n+d_k)=O(F_1(N)).$$

Theorem 1.2(II) can be improved by using the circle method. We shall consider a more generalized case. Let $2 \le Q \le N$, $k \ge 2$ be a fixed integer, $x \in \mathbb{Z}_Q$, and

$$R_k(x;Q,N) = \sum_{\substack{n_1=1 \\ n_1+\cdots+n_k \equiv x \,(\mathrm{mod}\, Q)}}^{N} \cdots \sum_{n_k=1}^{N} \lambda(n_1)\cdots\lambda(n_k).$$

Trivially we have $R_k(x;Q,N) \ll N^k Q^{-1}$. Let $A > 0$ be any fixed integer, and define

$$F_2(N) = \begin{cases} N(\log N)^{-A} & \text{unconditionally,} \\ N^{3/4+\varepsilon} & \text{under GRH.} \end{cases}$$

In Section 5 we shall prove the following theorem.

THEOREM 1.3. *For any $x \in \mathbb{Z}_N$ and $k \ge 3$, we have*

$$R_k(x;Q,N) = O(F_2(N)^{k-2} N^2 Q^{-1}).$$

If $k = 2$, then for all except $O(F_2(N)^2 Q N^{-2})$ elements x of $\mathbb{Z}_Q$, we have

$$R_2(x;Q,N) = O(F_2(N) N Q^{-1}).$$

For $S \subset \mathbb{Z}_N$, the indicator function χ_S of S is defined by

$$\chi_S(z) = \begin{cases} 1 & \text{if } z \in S, \\ 0 & \text{otherwise.} \end{cases}$$

Write $s = |S|$. We shall prove the following theorem in Section 5.

THEOREM 1.4. *Let $k \ge 3$ be any fixed integer. Define the following two properties of a set $S \subset \mathbb{Z}_N$:*

(R(k)) (k-representation) *For all except $o(N)$ elements x of $\mathbb{Z}_N$,*

$$\sum_{\substack{u_1=1 \\ u_1+\cdots+u_k \equiv x \,(\mathrm{mod}\, N)}}^{N} \cdots \sum_{u_k=1}^{N} \chi_S(u_1)\cdots\chi_S(u_k) = s^k/N + o(N^{k-1}).$$

(SR(k)) (Strong k-representation) *For all $x \in \mathbb{Z}_N$,*

$$\sum_{\substack{u_1=1 \\ u_1+\cdots+u_k \equiv x \,(\mathrm{mod}\, N)}}^{N} \cdots \sum_{u_k=1}^{N} \chi_S(u_1)\cdots\chi_S(u_k) = s^k/N + o(N^{k-1}).$$

For all subsets $S \subset \mathbb{Z}_N$, the above two properties are equivalent.

2. Proof of Theorem 1.1. In this section we assume the generalized Riemann hypothesis (GRH) to be true. First we list some well-known results in analytic number theory.

LEMMA 2.1. *Let $s = \sigma + it$ be a complex number, where $\sigma > 1/2$. For any character χ modulo q, we have*

$$\frac{1}{L(s,\chi)} \ll |qt|^{\varepsilon} \quad \text{and} \quad L(s,\chi) \ll |qt|^{\varepsilon}.$$

Proof. These estimates can be obtained by using the method of Chapter 14 in [21]. ∎

LEMMA 2.2. *For any character χ modulo q, we have*

$$\sum_{n \le x} \lambda(n)\chi(n) \ll x^{1/2+\varepsilon} q^{\varepsilon}.$$

Proof. Let

$$f(s) = \sum_{n=1}^{\infty} \frac{\lambda(n)\chi(n)}{n^s}.$$

By applying the Euler products we have

$$\begin{aligned}
f(s) &= \prod_p \left[1 + \frac{\lambda(p)\chi(p)}{p^s} + \cdots + \frac{\lambda(p^n)\chi(p^n)}{p^{ns}} + \cdots\right] \\
&= \prod_p \left[1 + \frac{(-1)\chi(p)}{p^s} + \cdots + \frac{(-1)^n\chi^n(p)}{p^{ns}} + \cdots\right] \\
&= \prod_p \frac{1}{1+\chi(p)/p^s} = \frac{L(2s,\chi^2)}{L(s,\chi)}.
\end{aligned}$$

Let $s_0 = \sigma_0 + it_0$, $b > 1$, $T \ge 1$ and $x \ge 1$. By the Perron formula we have

$$\begin{aligned}
\sum_{n \le x} \frac{\lambda(n)\chi(n)}{n^{s_0}} &= \frac{1}{2\pi i} \int_{b-iT}^{b+iT} f(s_0+s)\, \frac{x^s}{s}\, ds + O\bigg(\frac{x^b \zeta(b+\sigma_0)}{T}\bigg) \\
&\quad + O\bigg(x^{1-\sigma_0} \min\bigg(1, \frac{\log x}{T}\bigg)\bigg) + O(x^{-\sigma_0}).
\end{aligned}$$

Therefore

$$\sum_{n \le x} \lambda(n)\chi(n) = \frac{1}{2\pi i} \int_{b-iT}^{b+iT} \frac{L(2s,\chi^2)}{L(s,\chi)}\, \frac{x^s}{s}\, ds + O\bigg(\frac{x^b\zeta(b)}{T}\bigg) + O\bigg(\frac{x\log x}{T}\bigg).$$

Under GRH, we know that $L(s,\chi) \ne 0$ for $\operatorname{Re} s > 1/2$. Taking $b = 3/2$, we have

$$\sum_{n \le x} \lambda(n)\chi(n) = \frac{1}{2\pi i} \int_{3/2-iT}^{3/2+iT} \frac{L(2s,\chi^2)}{L(s,\chi)}\, \frac{x^s}{s}\, ds + O\bigg(\frac{x^{3/2}}{T}\bigg), \tag{2.1}$$

and

$$(2.2)\quad \frac{1}{2\pi i}\Big(\int_{3/2-iT}^{3/2+iT}+\int_{3/2+iT}^{1/2+\varepsilon+iT}+\int_{1/2+\varepsilon+iT}^{1/2+\varepsilon-iT}+\int_{1/2+\varepsilon-iT}^{3/2-iT}\Big)\frac{L(2s,\chi^2)}{L(s,\chi)}\,\frac{x^s}{s}\,ds=0.$$

Taking $T=x$, by Lemma 2.1 we get

$$(2.3)\quad \frac{1}{2\pi i}\int_{3/2+iT}^{1/2+\varepsilon+iT}\frac{L(2s,\chi^2)}{L(s,\chi)}\,\frac{x^s}{s}\,ds \ll \frac{(qT)^\varepsilon}{T}\int_{1/2+\varepsilon}^{3/2}x^\sigma\,d\sigma \ll \frac{(qT)^\varepsilon}{T}\,x^{3/2} \ll x^{1/2+\varepsilon}q^\varepsilon,$$

$$(2.4)\quad \frac{1}{2\pi i}\int_{1/2+\varepsilon+iT}^{1/2+\varepsilon-iT}\frac{L(2s,\chi^2)}{L(s,\chi)}\,\frac{x^s}{s}\,ds \ll x^{1/2+\varepsilon}\int_{-T}^{T}\frac{(q(|t|+1))^\varepsilon}{|t|+1}\,dt \ll (qT)^\varepsilon x^{1/2+\varepsilon} \ll x^{1/2+\varepsilon}q^\varepsilon,$$

and

$$(2.5)\quad \frac{1}{2\pi i}\int_{1/2+\varepsilon-iT}^{3/2-iT}\frac{L(2s,\chi^2)}{L(s,\chi)}\,\frac{x^s}{s}\,ds \ll \frac{(qT)^\varepsilon}{T}\int_{1/2+\varepsilon}^{3/2}x^\sigma\,d\sigma \ll \frac{(qT)^\varepsilon}{T}\,x^{3/2} \ll x^{1/2+\varepsilon}q^\varepsilon.$$

Then the conclusion follows from (2.1)–(2.5). ■

Now we prove Theorem 1.1. Let $a,b,t\in\mathbb{N}$ with $1\le a\le a+(t-1)b\le N$. If $b\ge N^{1/2}$, then

$$\sum_{j=0}^{t-1}\lambda(a+jb)=\sum_{\substack{n\le a+(t-1)b\\ n\equiv a\,(\mathrm{mod}\,b)}}\lambda(n)\ll\sum_{\substack{n\le N\\ n\equiv a\,(\mathrm{mod}\,b)}}1\ll N^{1/2}.$$

For $b<N^{1/2}$, let $d=(a,b)$. By Lemma 2.2 we have

$$\begin{aligned}\sum_{j=0}^{t-1}\lambda(a+jb)&=\sum_{\substack{n\le a+(t-1)b\\ n\equiv a\,(\mathrm{mod}\,b)}}\lambda(n)\\ &=\sum_{\substack{n\le a+(t-1)b\\ n/d\equiv a/d\,(\mathrm{mod}\,b/d)}}\lambda(n)=\sum_{\substack{n\le (a+(t-1)b)/d\\ n\equiv a/d\,(\mathrm{mod}\,b/d)}}\lambda(n)\lambda(d)\\ &=\frac{\lambda(d)}{\phi(b/d)}\sum_{\chi\,\mathrm{mod}\,b/d}\overline{\chi}\Big(\frac{a}{d}\Big)\sum_{n\le(a+(t-1)b)/d}\lambda(n)\chi(n)\ll N^{1/2+\varepsilon}.\end{aligned}$$

Therefore

$$W(L_N) = \max_{a,b,t} \Big| \sum_{j=0}^{t-1} \lambda(a+jb) \Big| \ll N^{1/2+\varepsilon}.$$

This proves Theorem 1.1.

3. Quasirandom subsets of $\mathbb{Z}_N$. In recent years, it has been discovered that there is a surprisingly large class $\Im$ of graph properties, all shared by quasirandom graphs, which are equivalent in the following sense: If a family of graphs has some property in $\Im$, then it must have all the properties in $\Im$. This is very surprising, since the properties may appear completely unrelated to one another. Quasirandom graphs, hypergraphs, set systems, subsets of $\mathbb{Z}_N$, and tournaments have been examined (see [5], [6] and [7] for details).

For $S \subset \mathbb{Z}_N$, the translate of S by x, denoted by $S + x$, is the set $\{z + x \mid z \in S\}$. For $S \subset \mathbb{Z}_N$, the graph G_S has vertex set $\mathbb{Z}_N$, and edge set $\{\{i,j\} \mid i + j \in S\}$. For subsets $S, T \subset \mathbb{Z}_N$, write $s = |S|$, $t = |T|$. F. R. K. Chung and R. L. Graham [6] listed a sequence of properties which a subset $S \subset \mathbb{Z}_N$ might possess, and showed that they are all equivalent. The primary result of [6] is the following.

PROPOSITION 3.1. *Define the following properties*:

(WT) (Weak translation) *For all except $o(N)$ elements x of $\mathbb{Z}_N$*,

$$|S \cap (S + x)| = s^2/N + o(N).$$

(ST) (Strong translation) *For all $T \subset \mathbb{Z}_N$ and all except $o(N)$ elements x of $\mathbb{Z}_N$*,

$$|S \cap (T + x)| = st/N + o(N).$$

(P(2)) (2-pattern) *For all except $o(N)$ elements u_1, u_2 of $\mathbb{Z}_N$*,

$$\sum_x \chi_S(x+u_1)\chi_S(x+u_2) = s^2/N + o(N).$$

(P(k)) (k-pattern) *For all except $o(N)$ elements $u_1, \ldots, u_k$ of $\mathbb{Z}_N$*,

$$\sum_x \prod_{i=1}^{k} \chi_S(x+u_i) = s^k/N^{k-1} + o(N).$$

(R(2)) (2-representation) *For all except $o(N)$ elements x of $\mathbb{Z}_N$*,

$$\sum_{u_1+u_2 \equiv x \pmod N} \chi_S(u_1)\chi_S(u_2) = s^2/N + o(N).$$

(R(k)) (k-representation) *For all except* $o(N)$ *elements* x *of* $\mathbb{Z}_N$,

$$\sum_{u_1+\cdots+u_k\equiv x\,(\mathrm{mod}\,N)}\prod_{i=1}^{k}\chi_S(u_i)=s^k/N+o(N^{k-1}).$$

(EXP) (Exponential sum) *For all* $j\neq 0$ *in* $\mathbb{Z}_N$,

$$\sum_{x\in\mathbb{Z}_N}\chi_S(x)e\bigg(\frac{jx}{N}\bigg)=o(N),\quad \textit{where}\quad e(y)=e^{2\pi iy}.$$

(GRAPH) (Quasirandom graph) *The graph* G_S *is quasirandom.*

(C($2t$)) ($2t$-cycle)

$$\sum_{x_1,\dots,x_{2t}}\chi_S(x_1+x_2)\chi_S(x_2+x_3)\cdots\chi_S(x_{2t-1}+x_{2t})\chi_S(x_{2t}+x_1)=s^{2t}+o(N^{2t}).$$

(DENSITY) (Relative density) *For all* $T\subset\mathbb{Z}_N$,

$$\sum_{x,y}\chi_T(x)\chi_T(y)\chi_S(x+y)=st^2/N+o(N^2).$$

For all subsets $S\subset\mathbb{Z}_N$, *the above properties are equivalent. Sets* S *which satisfy any one of the above conditions will be called* quasirandom.

As mentioned in [6], it is possible to replace all occurrences of $o(N)$ in Proposition 3.1 by explicit functions of N. We shall prove the following.

Theorem 3.1. *Let* $G(N)=o(N)$. *Define the following properties*:

(WT) (Weak translation) *For all except* $O(G(N))$ *elements* x *of* $\mathbb{Z}_N$,

$$|S\cap(S+x)|=s^2/N+O(G(N)).$$

(ST) (Strong translation) *For all* $T\subset\mathbb{Z}_N$ *and all except* $O(G(N))$ *elements* x *of* $\mathbb{Z}_N$,

$$|S\cap(T+x)|=st/N+O(G(N)).$$

(P(2)) (2-pattern) *For all except* $O(G(N))$ *elements* u_1,u_2 *of* $\mathbb{Z}_N$,

$$\sum_x\chi_S(x+u_1)\chi_S(x+u_2)=s^2/N+O(G(N)).$$

(P(k)) (k-pattern) *For all except* $O(G(N))$ *elements* $u_1,\dots,u_k$ *of* $\mathbb{Z}_N$,

$$\sum_x\prod_{i=1}^{k}\chi_S(x+u_i)=s^k/N^{k-1}+O(G(N)).$$

For all subsets $S\subset\mathbb{Z}_N$, *the above four properties are equivalent.*

Define the following properties:

(EXP) (Exponential sum) *For all* $j\neq 0$ *in* $\mathbb{Z}_N$,

$$\sum_{x\in\mathbb{Z}_N}\chi_S(x)e\bigg(\frac{jx}{N}\bigg)=O(G(N)^2/N).$$

(R(2)) (2-representation) *For all except $O(G(N))$ elements x of $\mathbb{Z}_N$,*

$$\sum_{u_1+u_2\equiv x \,(\mathrm{mod}\, N)} \chi_S(u_1)\chi_S(u_2) = s^2/N + O(G(N)).$$

(R(k)) (k-representation) *For all except $O(G(N))$ elements x of $\mathbb{Z}_N$,*

$$\sum_{u_1+\cdots+u_k\equiv x \,(\mathrm{mod}\, N)} \prod_{i=1}^{k} \chi_S(u_i) = s^k/N + O(N^{k-2}G(N)).$$

Sets S which satisfy (EXP) *also satisfy* (ST), (R(2)) *and* (R(k)).

Proof. We shall prove Theorem 3.1 according to the flowchart in Figure 3.1. Our proof follows the arguments in Theorem 3.1 of [6] with a slight modification. For completeness we give a detailed proof.

$$\begin{array}{ccccccc}
\mathrm{P}(2) & \overset{(3)}{\Rightarrow} & \mathrm{WT} & & & & \\
(2)\Uparrow & & (4)\Downarrow & & & & \\
\mathrm{P}(k) & \underset{(1)}{\Leftarrow} & \mathrm{ST} & \overset{(6)}{\Rightarrow} & \mathrm{R}(2) & \overset{(7)}{\Rightarrow} & \mathrm{R}(k) \\
 & & (5)\Uparrow & & & & \\
 & & \mathrm{EXP} & & & &
\end{array}$$

Fig. 3.1

(1) (ST) $\Rightarrow$ (P(k)).

For $k = 2$, (P(k)) follows at once from (ST) by taking $T = -S$. Now assume that (ST) $\Rightarrow$ (P(k)) for all values less than some $k \geq 3$. Let $u_1, \ldots, u_k \in \mathbb{Z}_N$, and define $T = \bigcap_{i=1}^{k-1}(S - u_i)$. Then $|T| = s^{k-1}/N^{k-2} + O(G(N))$. Applying (ST) to the sets S and T, we have

$$\begin{aligned}\sum_x \prod_{i=1}^{k} \chi_S(x+u_i) &= \Big|\bigcap_{i=1}^{k}(S-u_i)\Big| = |T\cap(S-u_k)| = |(T+u_k)\cap S| \\ &= s^k/N^{k-1} + O(G(N)).\end{aligned}$$

(2) (P(k)) $\Rightarrow$ (P(2)).

For $k = 2$, we immediately get (P(2)). Assume that (P(k)) $\Rightarrow$ (P(2)) for all values less than some $k \geq 3$. Then

$$\begin{aligned}&\sum_{u_1,\ldots,u_k} \Big(\sum_x \chi_S(x+u_1)\cdots\chi_S(x+u_k)\Big)^2 \\ &\qquad = \sum_{u_1,u_2}\sum_{u_3,\ldots,u_k} \Big(\sum_x \chi_S(x+u_1)\cdots\chi_S(x+u_k)\Big)^2\end{aligned}$$

$$\geq \sum_{u_1,u_2} \frac{1}{N^{k-2}} \Big(\sum_{u_3,\dots,u_k} \sum_x \chi_S(x+u_1)\cdots\chi_S(x+u_k) \Big)^2$$
$$= \sum_{u_1,u_2} \frac{1}{N^{k-2}} \Big(\sum_x \chi_S(x+u_1)\chi_S(x+u_2) \sum_{u_3,\dots,u_k} \chi_S(x+u_3)\cdots\chi_S(x+u_k) \Big)^2$$
$$= \sum_{u_1,u_2} \frac{1}{N^{k-2}} \Big(s^{k-2} \sum_x \chi_S(x+u_1)\chi_S(x+u_2) \Big)^2$$
$$= \frac{s^{2k-4}}{N^{k-2}} \sum_{u_1,u_2} \Big(\sum_x \chi_S(x+u_1)\chi_S(x+u_2) \Big)^2.$$

On the other hand, by (P(k)) we get

$$\sum_{u_1,\dots,u_k} \Big(\sum_x \chi_S(x+u_1)\cdots\chi_S(x+u_k) \Big)^2 = s^{2k}/N^{k-2} + O(N^{k+1}G(N)).$$

Thus,

$$\sum_{u_1,u_2} \Big(\sum_x \chi_S(x+u_1)\chi_S(x+u_2) \Big)^2 \leq s^4 + O(N^3 G(N)).$$

Since

$$\sum_{u_1,u_2} \sum_x \chi_S(x+u_1)\chi_S(x+u_2) = \sum_x \Big(\sum_{u_1} \chi_S(x+u_1) \Big) \Big(\sum_{u_2} \chi_S(x+u_2) \Big) = s^2 N,$$

we immediately get (P(2)).

(3) (P(2)) $\Rightarrow$ (WT).

From (P(2)) we know that, for all except $O(G(N))$ elements u_1, u_2 of $\mathbb{Z}_N$,

$$\sum_x \chi_S(x+u_1)\chi_S(x+u_2) = s^2/N + O(G(N)).$$

On the other hand,

$$\sum_x \chi_S(x+u_1)\chi_S(x+u_2) = \sum_y \chi_S(y)\chi_S(y+u_2-u_1) = |S \cap (S+u_2-u_1)|.$$

Thus (WT) follows.

(4) (WT) $\Rightarrow$ (ST).

Let $T \subset \mathbb{Z}_N$. By (WT), for all $a \in \mathbb{Z}_N$ and all except $O(G(N))$ elements b of $\mathbb{Z}_N$, we have $|(S-a) \cap (S-b)| = s^2/N + O(G(N))$. Thus,

$$\sum_{a\in T} \sum_{b \in T} |(S-a) \cap (S-b)| = s^2 t^2/N + O(N^2 G(N)),$$

so that

$$\begin{aligned}\sum_x |(S-x)\cap T|^2 &= \sum_x \Big(\sum_c \chi_S(x+c)\chi_T(c)\Big)^2\\ &= \sum_a\sum_b\sum_x \chi_S(x+a)\chi_S(x+b)\chi_T(a)\chi_T(b)\\ &= \sum_{a\in T}\sum_{b\in T} |(S-a)\cap(S-b)| = s^2t^2/N + O(N^2G(N)).\end{aligned}$$

Since

$$\begin{aligned}\sum_x |(S-x)\cap T| &= \sum_x\sum_a \chi_S(a+x)\chi_T(a)\\ &= \sum_a \chi_T(a)\sum_x \chi_S(a+x) = st,\end{aligned}$$

we have

$$|S\cap(T+x)| = |(S-x)\cap T| = st/N + O(G(N)).$$

(5) (EXP) $\Rightarrow$ (ST).

Define the matrix $M=(m_{ij})=(\chi_S(j-i))$. Then M has eigenvalues $\lambda_j=\sum_x \chi_S(x)e(jx/N)$, $j\in\mathbb{Z}_N$. Let $\lambda=\max_{j\neq 0}|\lambda_j|$. By (EXP), $\lambda=O(G(N)^2/N)$. Fix $T\subset\mathbb{Z}_N$ of size $t=|T|$. Define $\overline{1}=(1,\ldots,1)^{\mathrm{tr}}$ and

$$\overline{\chi}_T=(\chi_T(0),\ldots,\chi_T(N-1))^{\mathrm{tr}},\qquad \overline{V}_T=(V_T(0),\ldots,V_T(N-1))^{\mathrm{tr}},$$

where

$$V_T(i)=\frac{1}{N-t}\Big(-1+\frac{N}{t}\,\chi_S(i)\Big).$$

Thus,

$$\overline{\chi}_T=\frac{t(N-t)}{N}\Big(\frac{1}{N-t}\cdot\overline{1}+\overline{V}_T\Big)$$

and $\langle\overline{1},\overline{V}_T\rangle=0$. Also,

$$\|\overline{V}_T\|=\Big(\frac{1}{t}+\frac{1}{N-t}\Big)^{1/2},\qquad M\overline{\chi}_T=\frac{st}{N}\cdot\overline{1}+\frac{t(N-t)}{N}\,M\overline{V}_T.$$

Now suppose that for any $c>0$,

$$\sum_x \Big||S\cap(T+x)|-\frac{st}{N}\Big| > \frac{3cstG(N)}{N}. \tag{3.1}$$

Define

$$W=\Big\{y \,\Big|\, \Big||S\cap(T+y)|-\frac{st}{N}\Big| > \frac{cstG(N)}{N^2}\Big\}.$$

Then $w=|W|$ must satisfy $w>2csG(N)/N$, since otherwise

$$\sum_{y\in\mathbb{Z}_N}\left||S\cap(T+y)|-\frac{st}{N}\right|$$
$$=\sum_{y\in W}\left||S\cap(T+y)|-\frac{st}{N}\right|+\sum_{y\notin W}\left||S\cap(T+y)|-\frac{st}{N}\right|$$
$$\le wt+\frac{cstG(N)}{N^2}\cdot N\le\frac{3cstG(N)}{N},$$

which contradicts (3.1).

Assume without loss of generality that

$$W'=\left\{y\in W\,\middle|\,|S\cap(T+y)|>\frac{st}{N}+\frac{cstG(N)}{N^2}\right\}$$

satisfies $w'=|W'|>csG(N)/N$. Thus,

$$\sum_{y\in W'}|S\cap(T+y)|>w'st\left(\frac{1}{N}+\frac{cG(N)}{N^2}\right). \tag{3.2}$$

Let $W''=-W'$ and define

$$\overline{\chi}_{W''}=(\chi_{W''}(0),\dots,\chi_{W''}(N-1))^{\mathrm{tr}},\qquad \overline{V}_{W''}=(V_0'',\dots,V_{N-1}'')^{\mathrm{tr}},$$

where

$$V_i''=\frac{1}{N-t}\left(-1+\frac{N}{t}\,\chi_{W''}(i)\right).$$

As before,

$$\overline{\chi}_{W''}=\frac{w'(N-w')}{N}\left(\frac{1}{N-w'}\cdot\overline{1}+\overline{V}_{W''}\right)$$

with $\langle\overline{1},\overline{V}_{W''}\rangle=0$, and

$$\|\overline{V}_{W''}\|=\left(\frac{1}{w'}+\frac{1}{N-w'}\right)^{1/2}.$$

By (3.2) we have

$$\begin{aligned}\langle\overline{\chi}_{W''},M\overline{\chi}_T\rangle&=\sum_{i,j}\chi_{W''}(i)m_{ij}\chi_T(j)=\sum_{i,j}\chi_{W''}(i)\chi_S(j-i)\chi_T(j)\\&=\sum_{i\in W''}|T\cap(S+i)|\\&=\sum_{y\in W'}|S\cap(T+y)|>w'st\left(\frac{1}{N}+\frac{cG(N)}{N^2}\right).\end{aligned} \tag{3.3}$$

On the other hand,

$$(3.4)\quad \langle \overline{\chi}_{W''}, M\overline{\chi}_T\rangle = \left\langle \frac{w'}{N}\cdot\overline{1} + \frac{w'(N-w')}{N}\,\overline{V}_{W''}, \frac{st}{N}\cdot\overline{1} + \frac{t(N-t)}{N}\,M\overline{V}_T\right\rangle$$
$$= \frac{w'st}{N} + \frac{w'(N-w')t(N-t)}{N^2}\langle \overline{V}_{W''}, M\overline{V}_T\rangle$$
$$\le \frac{w'st}{N} + \frac{w'(N-w')t(N-t)}{N^2}\lambda\|\overline{V}_{W''}\|\cdot\|\overline{V}_T\|$$
$$= \frac{w'st}{N} + \frac{w'(N-w')t(N-t)}{N^2}\cdot O\biggl(\frac{G(N)^2}{N}\biggr)$$
$$\times\left(\frac{1}{t}+\frac{1}{n-t}\right)^{1/2}\left(\frac{1}{w'}+\frac{1}{n-w'}\right)^{1/2}$$
$$= \frac{w'st}{N} + \frac{(w'(N-w')t(N-t))^{1/2}}{N}\cdot O\biggl(\frac{G(N)^2}{N}\biggr)$$
$$= \frac{w'st}{N} + O\biggl(\frac{(w't)^{1/2}G(N)^2}{N}\biggr)$$
$$= \frac{w'st}{N} + O\biggl(\frac{w'st}{N}\cdot\frac{G(N)^{3/2}}{N^{3/2}c^{1/2}}\biggr).$$

Now from (3.3) and (3.4) we get $c \ll (G(N)/N)^{1/3}$, which is impossible, since c is arbitrary. Therefore

$$\sum_x \left| |S\cap(T+x)| - \frac{st}{N}\right| \ll \frac{stG(N)}{N}.$$

Thus we have $|S\cap(T+x)| = st/N + O(G(N))$.

(6) (ST) $\Rightarrow$ (R(2)).

Choose $T=-S$ in (ST), so that $\chi_T(z)=\chi_S(-z)$. Then

$$\sum_{x\in\mathbb{Z}_N}\chi_S(y)\chi_T(y-x) = \sum_y \chi_S(y)\chi_S(x-y) = s^2/N + O(G(N)),$$

which is just (R(2)).

(7) (R(2)) $\Rightarrow$ (R(k)).

For $k=2$, (R(2)) $\Rightarrow$ (R(k)) holds. Now assume it holds for all values less than some fixed value of $k\ge 3$. We have

$$\sum_x\Bigl(\sum_{u_1+\cdots+u_k=x}\chi_S(u_1)\cdots\chi_S(u_k)\Bigr)^2$$
$$= \sum_x\Bigl(\sum_{u_1+y=x}\chi_S(u_1)\sum_{u_2+\cdots+u_k=y}\chi_S(u_2)\cdots\chi_S(u_k)\Bigr)^2$$

$$= \sum_x \Big(\sum_y \chi_S(x-y) \sum_{u_2+\cdots+u_k=y} \chi_S(u_2)\cdots\chi_S(u_k)\Big)^2$$

$$= \sum_x \Big(\sum_y \chi_S(x-y)(s^{k-1}/N + O(N^{k-3}G(N)))\Big)^2 + O(N^{2k-3}G(N)^2)$$

$$= \sum_x \Big(\sum_y \chi_S(x-y)\Big)^2 (s^{2k-2}/N^2 + O(N^{2k-5}G(N))) + O(N^{2k-3}G(N)^2)$$

$$= s^{2k}/N + O(N^{2k-2}G(N)).$$

Since

$$\sum_x \sum_{u_1+\cdots+u_k=x} \chi_S(u_1)\cdots\chi_S(u_k)$$

$$= \sum_x \sum_{u_1} \cdots \sum_{u_{k-1}} \chi_S(u_1)\cdots\chi_S(u_{k-1})\chi_S(x-u_1-\cdots-u_{k-1})$$

$$= \sum_{u_1} \cdots \sum_{u_{k-1}} \chi_S(u_1)\cdots\chi_S(u_{k-1}) \sum_x \chi_S(x-u_1-\cdots-u_{k-1}) = s^k,$$

we have $\sum_{u_1+\cdots+u_k=x} \chi_S(u_1)\cdots\chi_S(u_k) = s^k/N + O(N^{k-2}G(N))$. ■

4. Proof of Theorem 1.2. Now we shall use Theorem 3.1 to study the pseudorandomness of the Liouville function $\lambda(n)$. We need the following lemma.

LEMMA 4.1.

(I) *For any real number $H > 0$ and $x > x_0(H)$, we have*

$$\Big|\sum_{n\le x} \lambda(n)e(n\alpha)\Big| < x(\log x)^{-H} \quad \textit{for all } 0 \le \alpha \le 1.$$

(II) *Under GRH, for $\varepsilon > 0$ and $x > x_1(\varepsilon)$, we have*

$$\Big|\sum_{n\le x} \lambda(n)e(n\alpha)\Big| < x^{3/4+\varepsilon} \quad \textit{for all } 0 \le \alpha \le 1.$$

Proof. Part (I) is Lemma 2 of [19], and (II) is the Theorem of [1]. ■

Now we prove Theorem 1.2. Recall that

$$\lambda'(n) = \begin{cases} \lambda(n) & \text{if } 1 \le n \le N,\\ \lambda(n-N) & \text{if } N+1 \le n \le 2N \end{cases}$$

and set

$$S = \{n \mid \lambda'(n) = 1, 1 \le n \le N\} \subset \mathbb{Z}_N.$$

Let $A > 0$ be any fixed integer, recall that

$$F_1(N) = \begin{cases} N(\log N)^{-A} & \text{unconditionally,} \\ N^{7/8+\varepsilon} & \text{under GRH,} \end{cases}$$

and define

$$F_2(N) = \begin{cases} N(\log N)^{-A} & \text{unconditionally,} \\ N^{3/4+\varepsilon} & \text{under GRH.} \end{cases}$$

It is obvious that

$$F_1(N) = O(N^{1/2} F_2(N)^{1/2}).$$

By Lemma 4.1 we easily get

$$s = |S| = \sum_{\substack{n=1 \\ \lambda'(n)=1}}^{N} 1 = \sum_{\substack{n=1 \\ \lambda(n)=1}}^{N} 1 = \frac{1}{2}\sum_{n=1}^{N}(\lambda(n)+1) = \frac{N}{2} + \frac{1}{2}\sum_{n=1}^{N}\lambda(n)$$
$$= \frac{N}{2} + O(F_2(N)).$$

For all $j \neq 0$ in $\mathbb{Z}_N$, we have

$$\sum_{n\in\mathbb{Z}_N} \chi_S(n) e\left(\frac{jn}{N}\right) = \sum_{\substack{n=1 \\ \lambda(n)=1}}^{N} e\left(\frac{jn}{N}\right) = \frac{1}{2}\sum_{n=1}^{N}(\lambda(n)+1) e\left(\frac{jn}{N}\right)$$
$$= \frac{1}{2}\sum_{n=1}^{N}\lambda(n) e\left(\frac{jn}{N}\right) = O(F_2(N)).$$

Then from Theorem 3.1 we know that for all except $O(F_1(N))$ elements u_1, u_2 of $\mathbb{Z}_N$,

$$\sum_{n\in\mathbb{Z}_N} \chi_S(n+u_1)\chi_S(n+u_2) = \frac{s^2}{N} + O(F_1(N)) = \frac{N}{4} + O(F_1(N)), \tag{4.1}$$

and for all except $O(F_1(N))$ elements $u_1, \ldots, u_k$ of $\mathbb{Z}_N$,

$$\sum_{n\in\mathbb{Z}_N} \chi_S(n+u_1)\cdots\chi_S(n+u_k) = \frac{s^k}{N^{k-1}} + O(F_1(N)) \tag{4.2}$$
$$= \frac{N}{2^k} + O(F_1(N)).$$

Noting that

$$\sum_{n\in\mathbb{Z}_N}\chi_S(n+u_1)\chi_S(n+u_2)=\sum_{\substack{n=1\\ \lambda'(n+u_1)=1\\ \lambda'(n+u_2)=1}}^{N}1 \tag{4.3}$$

$$=\frac{1}{4}\sum_{n=1}^{N}(\lambda'(n+u_1)+1)(\lambda'(n+u_2)+1)$$

$$=\frac{1}{4}\sum_{n=1}^{N}\lambda'(n+u_1)\lambda'(n+u_2)+\frac{1}{4}\sum_{n=1}^{N}\lambda'(n+u_1)+\frac{1}{4}\sum_{n=1}^{N}\lambda'(n+u_2)+\frac{N}{4},$$

from Lemma 4.1, (4.1) and (4.3) we get

$$\sum_{n=1}^{N}\lambda'(n+u_1)\lambda'(n+u_2)=O(F_1(N)).$$

Now suppose that for all except $O(F_1(N))$ elements $u_1,\dots,u_{k-1}$ of $\mathbb{Z}_N$,

$$\sum_{n=1}^{N}\lambda'(n+u_1)\cdots\lambda'(n+u_{k-1})=O(F_1(N)).$$

Then we have

$$\sum_{n\in\mathbb{Z}_N}\chi_S(n+u_1)\cdots\chi_S(n+u_k)=\sum_{\substack{n=1\\ \lambda'(n+u_1)=1\\ \cdots\\ \lambda'(n+u_k)=1}}^{N}1 \tag{4.4}$$

$$=\frac{1}{2^k}\sum_{n=1}^{N}(\lambda'(n+u_1)+1)\cdots(\lambda'(n+u_k)+1)$$

$$=\frac{1}{2^k}\sum_{n=1}^{N}\lambda'(n+u_1)\cdots\lambda'(n+u_k)+\frac{1}{2^k}\sum_{n=1}^{N}1+O(F_1(N)).$$

Combining (4.2) and (4.4), we get

$$\sum_{n=1}^{N}\lambda'(n+u_1)\cdots\lambda'(n+u_k)=O(F_1(N))$$

for all except $O(F_1(N))$ elements $u_1,\dots,u_k$ of $\mathbb{Z}_N$.

Using similar methods and Theorem 3.1 we obtain

$$\sum_{\substack{n_1=1\\ n_1+\cdots+n_k\equiv x \,(\mathrm{mod}\, N)}}^{N}\cdots\sum_{n_k=1}^{N}\lambda(n_1)\cdots\lambda(n_k)=O(N^{k-2}F_1(N))$$

for all except $O(F_1(N))$ elements x of $\mathbb{Z}_N$. This proves Theorem 1.2.

5. Proof of Theorems 1.3 and 1.4. We need the following lemmas.

LEMMA 5.1. *Let $Q \ge 2$ be an integer. Then*

$$\frac{1}{Q}\sum_{a=1}^{Q} e\left(\frac{ar}{Q}\right) = \begin{cases} 1 & \text{if } r \equiv 0 \pmod{Q}, \\ 0 & \text{if } r \not\equiv 0 \pmod{Q}. \end{cases}$$

LEMMA 5.2 (Parseval's identity). *Let $Q \ge 2$ be an integer and $f : \mathbb{Z}_Q \to \mathbb{C}$ be any function. If there exists a function $g : \mathbb{Z}_Q \to \mathbb{C}$ such that*

$$f(x) = \sum_{j=1}^{Q} g(j) e\left(-\frac{jx}{Q}\right), \quad x \in \mathbb{Z}_Q,$$

then

$$\sum_{x=1}^{Q} |f(x)|^2 = Q \sum_{x=1}^{Q} |g(x)|^2.$$

Proof. By Lemma 5.1 we get

$$\begin{aligned}\sum_{x=1}^{Q} |f(x)|^2 &= \sum_{x=1}^{Q}\sum_{j_1=1}^{Q}\sum_{j_2=1}^{Q} \overline{g(j_1)}\, g(j_2) e\left(\frac{x(j_1-j_2)}{Q}\right) \\ &= \sum_{j_1=1}^{Q}\sum_{j_2=1}^{Q} \overline{g(j_1)}\, g(j_2) \sum_{x=1}^{Q} e\left(\frac{x(j_1-j_2)}{Q}\right) = Q\sum_{j=1}^{Q} |g(j)|^2. \quad \blacksquare\end{aligned}$$

Now we prove Theorem 1.3. By Lemma 5.1 we have

$$\begin{aligned} R_k(x;Q,N) &= \sum_{\substack{n_1=1 \\ n_1+\cdots+n_k \equiv x \,(\mathrm{mod}\, Q)}}^{N} \cdots \sum_{n_k=1}^{N} \lambda(n_1)\cdots\lambda(n_k) \\ &= \frac{1}{Q}\sum_{n_1=1}^{N}\cdots\sum_{n_k=1}^{N} \lambda(n_1)\cdots\lambda(n_k)\sum_{a=1}^{Q} e\left(\frac{a(n_1+\cdots+n_k-x)}{Q}\right) \\ &= \frac{1}{Q}\sum_{a=1}^{Q} e\left(-\frac{ax}{Q}\right)\sum_{n_1=1}^{N}\lambda(n_1)e\left(\frac{an_1}{N}\right)\cdots\sum_{n_k=1}^{N}\lambda(n_k)e\left(\frac{an_k}{N}\right) \\ &= \frac{1}{Q}\sum_{a=1}^{Q} e\left(-\frac{ax}{Q}\right)\left(\sum_{n=1}^{N}\lambda(n)e\left(\frac{an}{N}\right)\right)^k \\ &= \frac{1}{Q}\sum_{a=1}^{Q} e\left(-\frac{ax}{Q}\right) S^k(a,N), \end{aligned}$$

say, where $S(a,N)=\sum_{n=1}^{N}\lambda(n)e(an/N)$. So we have

$$\begin{aligned}R_k(x;Q,N) &\ll \frac{1}{Q}\sum_{a=1}^{Q}|S(a,N)|^k \\ &\ll \max_{1\le b\le Q}|S(b,N)|^{k-2}\frac{1}{Q}\sum_{a=1}^{Q}|S(a,N)|^2.\end{aligned}\tag{5.1}$$

By Lemma 5.1 we have

$$\begin{aligned}\frac{1}{Q}\sum_{a=1}^{Q}|S(a,N)|^2 &= \frac{1}{Q}\sum_{a=1}^{Q}\sum_{n_1=1}^{N}\sum_{n_2=1}^{N}\lambda(n_1)\lambda(n_2)e\Big(\frac{a(n_1-n_2)}{Q}\Big) \\ &= \sum_{n_1=1}^{N}\sum_{n_2=1}^{N}\lambda(n_1)\lambda(n_2)\frac{1}{Q}\sum_{a=1}^{Q}e\Big(\frac{a(n_1-n_2)}{Q}\Big) \\ &\ll \sum_{\substack{1\le n_1,n_2\le N\\ n_1-n_2\equiv 0\ (\mathrm{mod}\ Q)}} 1 \ll N^2Q^{-1}.\end{aligned}\tag{5.2}$$

Let $A>0$ be any fixed integer, and recall that

$$F_2(N)=\begin{cases} N(\log N)^{-A} & \text{unconditionally,}\\ N^{3/4+\varepsilon} & \text{under GRH.}\end{cases}$$

From Lemma 4.1 we know that

$$|S(b,N)|=O(F_2(N)) \quad \text{for all } b.\tag{5.3}$$

Now the case $k\ge 3$ of Theorem 1.3 follows from (5.1)–(5.3).

For $k=2$, by Lemma 5.2, (5.2) and (5.3) we have

$$\begin{aligned}\sum_{x=1}^{Q}|R_2(x;Q,N)|^2 &= Q^{-1}\sum_{a=1}^{Q}|S(a,N)|^4 \\ &\ll \max_{1\le b\le Q}|S(b,N)|^2\frac{1}{Q}\sum_{a=1}^{Q}|S(a,N)|^2 \\ &\ll F_2(N)^2N^2Q^{-1}.\end{aligned}$$

Hence the case $k=2$ of Theorem 1.3 follows.

Now we prove Theorem 1.4. By Proposition 3.1 we know that (EXP) $\Leftrightarrow$ (R(k)). It is obvious that (SR(k)) $\Rightarrow$ (R(k)). Thus we only need to prove that (EXP) $\Rightarrow$ (SR(k)).

By Lemma 5.1 we have

$$\begin{aligned}
&\sum_{\substack{u_1=1 \\ u_1+\cdots+u_k\equiv x \,(\mathrm{mod}\, N)}}^{N} \cdots \sum_{u_k=1}^{N} \chi_S(u_1)\cdots\chi_S(u_k) \\
&\qquad = \frac{1}{N}\sum_{u_1=1}^{N}\cdots\sum_{u_k=1}^{N}\chi_S(u_1)\cdots\chi_S(u_k)\sum_{a=1}^{N} e\Big(\frac{a(u_1+\cdots+u_k-x)}{N}\Big) \\
&\qquad = \frac{1}{N}\sum_{a=1}^{N} e\Big(-\frac{ax}{N}\Big)\Big(\sum_{u=1}^{N}\chi_S(u)e\Big(\frac{au}{N}\Big)\Big)^k \\
&\qquad = s^k/N + \frac{1}{N}\sum_{a=1}^{N-1} e\Big(-\frac{ax}{N}\Big)\Big(\sum_{u=1}^{N}\chi_S(u)e\Big(\frac{au}{N}\Big)\Big)^k.
\end{aligned}$$

It is easy to show that

$$\begin{aligned}
\frac{1}{N}\sum_{a=1}^{N-1} e\Big(-\frac{ax}{N}\Big)\Big(\sum_{u=1}^{N}\chi_S(u)e\Big(\frac{au}{N}\Big)\Big)^k &\ll \frac{1}{N}\sum_{a=1}^{N-1}\Big|\sum_{u=1}^{N}\chi_S(u)e\Big(\frac{au}{N}\Big)\Big|^k \\
&\ll \max_{1\le b\le N-1}\Big|\sum_{u=1}^{N}\chi_S(u)e\Big(\frac{bu}{N}\Big)\Big|^{k-2}\cdot\frac{1}{N}\sum_{a=1}^{N-1}\Big|\sum_{u=1}^{N}\chi_S(u)e\Big(\frac{au}{N}\Big)\Big|^2.
\end{aligned}$$

Noting that

$$\sum_{u=1}^{N}\chi_S(u)e\Big(\frac{bu}{N}\Big) = o(N) \quad \text{for all } b\ne 0 \text{ in } \mathbb{Z}_N,$$

and

$$\begin{aligned}
\frac{1}{N}\sum_{a=1}^{N-1}\Big|\sum_{u=1}^{N}\chi_S(u)e\Big(\frac{au}{N}\Big)\Big|^2 &= \frac{1}{N}\sum_{a=1}^{N}\Big|\sum_{u=1}^{N}\chi_S(u)e\Big(\frac{au}{N}\Big)\Big|^2 - \frac{s^2}{N} \\
&= \frac{1}{N}\sum_{u_1=1}^{N}\chi_S(u_1)\sum_{u_2=1}^{N}\chi_S(u_2)\sum_{a=1}^{N}e\Big(\frac{a(u_1-u_2)}{N}\Big) - \frac{s^2}{N} \\
&= \sum_{u=1}^{N}\chi_S(u)^2 - \frac{s^2}{N} = s - \frac{s^2}{N},
\end{aligned}$$

we conclude that

$$\sum_{\substack{u_1=1 \\ u_1+\cdots+u_k\equiv x \,(\mathrm{mod}\, N)}}^{N} \cdots \sum_{u_k=1}^{N} \chi_S(u_1)\cdots\chi_S(u_k) = s^k/N + o(N^{k-1}) \quad \text{for all } x\in\mathbb{Z}_N.$$

This completes the proof of Theorem 1.4.

6. Conclusion. In this paper, the pseudorandomness of the Liouville function has been studied, and some estimates were obtained. Furthermore, we studied quasirandom properties of subsets of $\mathbb{Z}_N$. As mentioned in [6], it is natural to explore the possible links of these ideas to pseudorandom sequences. We hope to do this soon in a forthcoming paper.

Acknowledgments. Portions of this paper were completed while the first author was visiting the ergodic prime number theory seminar supported by Morningside Center of Mathematics, and he would like to thank Chaohua Jia and Yonghui Wang for inviting him to attend this seminar. He would also like to thank Yonghui Wang for helpful conversations.

This research was supported by the National Grand Fundamental Research 973 Programs of China (Grants 2007CB807902 and 2007CB807903), the National Natural Science Foundation of China (Grants No. 10671155 and No. 10771027); and the Natural Science Foundation of Shaanxi province of China (Grant No. 2006A04).

References

[1] R. C. Baker and G. Harman, *Exponential sums formed with the Möbius function*, J. London Math. Soc. 43 (1991), 193–198.

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

[3] —, —, —, —, —, *On finite pseudorandom binary sequences IV: The Liouville function, II*, ibid. 95 (2000), 343–359.

[4] J. Cassaigne, C. Mauduit and A. Sárközy, *On finite pseudorandom binary sequences VII: The measures of pseudorandomness*, ibid. 103 (2002), 97–118.

[5] F. R. K. Chung and R. L. Graham, *Quasi-random set systems*, J. Amer. Math. Soc. 4 (1991), 151–196.

[6] —, —, *Quasi-random subsets of $\mathbb{Z}_n$*, J. Combin. Theory Ser. A 61 (1992), 64–86.

[7] F. R. K. Chung, R. L. Graham and R. M. Wilson, *Quasi-random graphs*, Combinatorica 9 (1989), 345–362.

[8] P. D. T. A. Elliott, *On the correlation of multiplicative functions*, Notas Soc. Mat. Chile 11 (1992), 1–11.

[9] E. Fouvry, P. Michel, J. Rivat and A. Sárközy, *On the pseudorandomness of the signs of Kloosterman sums*, J. Austral. Math. Soc. 77 (2004), 425–436.

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

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

[12] —, *Pseudorandom sequences constructed by the power generator*, ibid. 52 (2006), 9–26.

[13] G. Harman, J. Pintz and D. Wolke, *A note on the Möbius and the Liouville function*, Studia Sci. Math. Hungar. 20 (1985), 295–299.

[14] H. N. Liu, *New pseudorandom sequences constructed using multiplicative inverses*, Acta Arith. 125 (2006), 11–19.

[15] S. R. Louboutin, J. Rivat and A. Sárközy, *On a problem of D. H. Lehmer*, Proc. Amer. Math. Soc. 135 (2007), 969–975.

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

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

[18] —, —, *Construction of pseudorandom binary sequences by using the multiplicative inverse*, Acta Math. Hungar. 108 (2005), 239–252.

[19] A. Sárközy, *On the number of prime factors of integers of the form* $a_i + b_j$, Studia Sci. Math. Hungar. 23 (1988), 161–168.

[20] —, *A finite pseudorandom binary sequence*, ibid. 38 (2001), 377–384.

[21] E. C. Titchmarsh, *The Theory of the Riemann Zeta-Function*, Oxford Univ. Press, Oxford, 1986.

Department of Mathematics
Northwest University
Xi'an, Shaanxi, P.R. China
E-mail: hnliumath@hotmail.com

College of Mathematics Science
Shandong Normal University
Jinan, Shandong, P.R. China
E-mail: zhaiwg@hotmail.com

Received on 20.9.2007
and in revised form on 25.8.2008 (5529)