633-3

TM-1042/203/00

TECHNICAL MEMORANDUM

(TM Series)

This document was produced by SDC in performance of U. S. Government Contracts

The Autocorrelation and Joint Distribution Functions of the Sequences, $\{\frac{a}{m} j^2\}$, $\{\frac{a}{m}(j+\tau)^2\}$

by

D. L. Jagerman

March 15, 1963

SYSTEM DEVELOPMENT CORPORATION
2500 COLORADO AVE.
SANTA MONICA
CALIFORNIA

THE AUTOCORRELATION AND JOINT DISTRIBUTION FUNCTIONS OF THE SEQUENCES, $\{\frac{a}{m} j^2\}$, $\{\frac{a}{m}(j+\tau)^2\}$

by

D. L. Jagerman

1. INTRODUCTION

The present-day extensive use of Monte Carlo procedures necessitates the careful investigation of methods for the generation of random numbers. In its simplest form, the underlying principle of all Monte Carlo procedures finds its expression in the following theorem.[1]

THEOREM: Let $(x_j)_1^\infty$ be a sequence equidistributed over (0,1), and let f(x) be a function Riemann integrable on (0,1); then

$$\sum_{j=1}^{N} f(x_j) \sim N\int_0^1 f(x)dx \ .$$

Thus, the theorem states that sample averages approximate the value of an integral. It is to be noted that the only property of the sequence $(x_j)_1^\infty$ employed is its equidistribution.

In applications, one may employ several equidistributed sequences simultaneously; accordingly, new requirements may arise. The sequences may be employed, for example, as bases for decision, in which case it may be required that they be independent. Thus, depending on the Monte Carlo problem considered, equidistributed sequences may be required to possess other random-number character-

istics. Let the sequences $(x_j)_1^\infty$, $(x_{j+\tau})_1^\infty$ be designated respectively by x, $x^{(\tau)}$, in which τ is a non-zero integer, then an additional desirable characteristic is the statistical independence of x, $x^{(\tau)}$. A sequence exhibiting such characteristics is $(\{\alpha j^2\})_1^\infty$ in which α is an irrational number.[2] The symbol $\{x\}$ is employed to designate the fractional part of x.

However, from the viewpoint of the practical utilization of the sequence suggested above by means of a digital computer, it is necessary to replace α by a rational number, and, hence, to lose some of the precision with which the characteristics discussed above are satisfied. Accordingly, the sequences which will be studied are

$$x = (\{\tfrac{a}{m} j^2\})_o^{m-1}, \quad x^{(\tau)} = (\{\tfrac{a}{m}(j+\tau)^2\})_o^{m-1} .$$

The integers a, m are taken relatively prime. Of particular interest will be the deviation of the characteristics of these sequences from the ideal random-number characteristics.

Let $\rho(x)$ be given by $\rho(x) = \frac{1}{2} - \{x\}$; then the autocorrelation function $\psi(\tau)$ of a sequence $(x_j)_1^\infty$ is defined by

$$\psi(\tau) = \lim_{N\to\infty} \frac{1}{N} \sum_{j=1}^{N} \rho(x_j)\ \rho(x_{j+\tau}) .$$

For the sequence to be studied, this takes the form

$$\psi(\tau) = \frac{1}{m} \sum_{j=0}^{m-1} \rho(\tfrac{a}{m} j^2)\ \rho(\tfrac{a}{m}(j+\tau)^2) .$$

It will be shown that, uniformly in τ for the range

$$1 \leq \tau < \sqrt{m} ,$$

the autocorrelation function is small; that is, quantatively,

$$|\psi(\tau)| < m^{-\frac{1}{2}[\frac{2}{3}(2+\sqrt{2})^{\nu(m)} \ln^2 m + 30 \cdot 2^{\nu(m)} \ln m]} ,$$

provided $(a,m) = 1$ and $m \geq 36$. The function $\nu(m)$ is the number of distinct prime divisors of m. Thus, the sequence $(\{\frac{a}{m} j^2\})_0^{m-1}$ is approximately uncorrelated.

Let $H_\alpha(x)$ be given by $H_\alpha(x) = \alpha + \rho(x) - \rho(x-\alpha)$; then the joint distribution function $G(\alpha,\beta)$ of the sequences x, $x^{(\tau)}$ is given by

$$G(\alpha,\beta) = \lim_{N\to\infty} \frac{1}{N} \sum_{j=1}^{N} H_\alpha(x_j) \, H_\beta(x_{j+\tau}) .$$

For the sequence $(\{\frac{a}{m} j^2\})_0^{m-1}$, this takes the form

$$G(\alpha,\beta) = \frac{1}{m} \sum_{j=0}^{m-1} H_\alpha(\{\tfrac{a}{m} j^2\}) \, H_\beta(\{\tfrac{a}{m}(j+\tau)^2\}) .$$

It will be shown that, uniformly in τ for the same range stated above, and under the same conditions on a, m,

$$|G(\alpha,\beta) - \alpha\beta| < m^{-\frac{1}{2}} (2+\sqrt{2})^{\nu(m)} (\tfrac{8}{3} \ln^2 m + 88 \ln m) .$$

Thus, the sequences $(\{\frac{a}{m} j^2\})_0^{m-1}$, $(\{\frac{a}{m}(j+\tau)^2\})_0^{m-1}$ are approximately independently equidistributed over (0,1).

The above enumerated properties show the possible applicability of the sequences $(\{\frac{a}{m} j^2\})_o^{m-1}$, $(\{\frac{a}{m}(j+\tau)^2\})_o^{m-1}$ as random numbers in Monte Carlo procedures. However, an important question is the behavior, from the viewpoint of random-number characteristics, of consecutive portions of the complete sequences. This is being studied by the author, and an investigation of the question will appear in another paper.

2. ANALYTICAL DISCUSSION

The proofs of the main theorems require the establishment of several lemmas.

Lemma 1: $t \geq 1$, $|\eta| < 1$

$$\Longrightarrow \quad \rho(x) = \sum_{1 \leq h \leq t} \frac{\sin 2\pi hx}{\pi h} + \eta \min\left(1, \frac{1}{2\pi t\|x\|}\right),$$

in which $\|x\|$ denotes the distance from x to the nearest integer. It is understood that when x is an integer, the estimate 1 is used.

Proof: The Fourier series for $\rho(x)$ is

$$\rho(x) = \sum_{h=1}^{\infty} \frac{\sin 2\pi hx}{\pi h}; \tag{1}$$

hence, it may be necessary to establish

$$\left| \sum_{h>t} \frac{\sin 2\pi hx}{\pi h} \right| < \min\left(1, \frac{1}{2\pi t\|x\|}\right). \tag{2}$$

The following standard theorem derived from Abel's transformation of series will be used:

$$a_{\ell\downarrow} \geq 0, \quad \left| \sum_{p=M}^{\ell} b_p \right| \leq B \tag{3}$$

$$\Longrightarrow \left| \sum_{\ell=M}^{n} a_\ell b_\ell \right| \leq a_M B .$$

Also standard is the following estimate:

$$\left| \sum_{p=M}^{\ell} \sin 2\pi px \right| \leq \frac{1}{2\|x\|} . \tag{4}$$

Applying the inequalities of Equations (3) and (4), one has

$$\left| \sum_{h>t} \frac{\sin 2\pi hx}{\pi h} \right| \leq \frac{1}{2\pi([t]+1)\|x\|} < \frac{1}{2\pi t\|x\|} . \tag{5}$$

If $2\pi t\|x\| > 1$, then Equation (2) has been established. Consider now the case $2\pi t\|x\| \leq 1$; then

$$\sum_{h>t} \frac{\sin 2\pi hx}{\pi h} = \sum_{h=1}^{\infty} \frac{\sin 2\pi hx}{\pi h} - \sum_{1 \leq h \leq t} \frac{\sin 2\pi hx}{\pi h} . \tag{6}$$

Thus

$$\left| \sum_{h>t} \frac{\sin 2\pi hx}{\pi h} \right| \leq \frac{1}{2} + \left| \sum_{1 \leq h \leq t} \frac{\sin 2\pi hx}{\pi h} \right| \tag{7}$$

$$\leq \frac{1}{2} + \sum_{1 \leq h \leq t} \frac{|\sin 2\pi h\|x\||}{\pi h} \leq \frac{1}{2} + 2\|x\|t \leq \frac{1}{2} + \frac{1}{\pi} < 1 .$$

Equation (2) is now established. The Fourier series for $\rho(x)$ does not equal $\rho(x)$ when x is an integer; however, with the understanding stated in the lemma, the lemma remains correct also in this case.

Lemma 2: $\left| \sum_{1 \le h \le t} \frac{\sin 2\pi hx}{\pi h} \right| < \frac{3}{2}$.

Proof: One has

$$\sum_{1 \le h \le t} \frac{\sin 2\pi hx}{\pi h} = \sum_{h=1}^{\infty} \frac{\sin 2\pi hx}{\pi h} - \sum_{h>t} \frac{\sin 2\pi hx}{\pi h} . \tag{8}$$

Hence,

$$\left| \sum_{1 \le h \le t} \frac{\sin 2\pi hx}{\pi h} \right| \le \frac{1}{2} + \left| \sum_{h>t} \frac{\sin 2\pi hx}{\pi h} \right| < \frac{3}{2} . \tag{9}$$

The inequality of Lemma 1 was used.

Lemma 3: $t \ge 1$, $|\eta| < 1$

$$\Longrightarrow \rho(x)\rho(y) = \sum_{1 \le h \le t} \sum_{1 \le \ell \le t} \frac{\sin 2\pi hx \cdot \sin 2\pi \ell y}{\pi^2 h\ell} +$$

$$\frac{5}{2}\eta\left[\min\left(1, \frac{1}{2\pi t\|x\|}\right) + \min\left(1, \frac{1}{2\pi t\|y\|}\right)\right] .$$

Proof: Use of Lemma 1 yields

$$\rho(x)\rho(y) = \sum_{1 \le h \le t} \sum_{1 \le \ell \le t} \frac{\sin 2\pi hx \cdot \sin 2\pi \ell y}{\pi^2 h\ell} +$$

$$\eta \sum_{1 \le h \le t} \frac{\sin 2\pi hx}{\pi h} \cdot \min\left(1, \frac{1}{2\pi t\|y\|}\right) +$$

$$\eta \sum_{1 \le \ell \le t} \frac{\sin 2\pi \ell y}{\pi \ell} \cdot \min\left(1, \frac{1}{2\pi t\|x\|}\right) + \tag{10}$$

$$\eta^2 \min\left(1, \frac{1}{2\pi t\|x\|}\right) \min\left(1, \frac{1}{2\pi t\|y\|}\right) .$$

Lemma 2 allows one to write

$$\rho(x)\rho(y) = \sum_{1 \le h \le t} \sum_{1 \le \ell \le t} \frac{\sin 2\pi hx \cdot \sin 2\pi \ell y}{\pi^2 h\ell} +$$

$$\frac{3}{2}\eta\left[\min\left(1, \frac{1}{2\pi t\|x\|}\right) + \min\left(1, \frac{1}{2\pi t\|y\|}\right)\right] + \tag{11}$$

$$\eta^2 \min\left(1, \frac{1}{2\pi t\|x\|}\right) \min\left(1, \frac{1}{2\pi t\|y\|}\right) .$$

Observing that

$$\min\left(1, \frac{1}{2\pi t\|x\|}\right) \min\left(1, \frac{1}{2\pi t\|y\|}\right) \le \min\left(1, \frac{1}{2\pi t\|x\|}\right) \le$$

$$\min\left(1, \frac{1}{2\pi t\|x\|}\right) + \min\left(1, \frac{1}{2\pi t\|y\|}\right) \tag{12}$$

the lemma follows.

Let f(j), g(j) be given functions of the integral variable j. Define e(x) by

$$e(x) = e^{i2\pi x} , \tag{13}$$

R by

$$R = \sum_{a < j \le b} \rho(f(j))\rho(g(j)) , \tag{14}$$

$S_{h,\ell}$ by

$$S_{h,\ell} = \sum_{a < j \leq b} e(hf(j) + \ell g(j)) , \tag{15}$$

and S_f by

$$S_f = \sum_{a < j \leq b} \min\left(1, \frac{1}{2\pi t\|f(j)\|}\right) ; \tag{16}$$

then

Lemma 4: $t \geq 1$

$$\Rightarrow \quad \left|R\right| < \frac{1}{2\pi^2} \sum_{1 \leq h \leq t} \sum_{1 \leq \ell \leq t} \frac{\left|S_{h,\ell}\right|}{h\ell} + \frac{1}{2\pi^2} \sum_{1 \leq h \leq t} \sum_{1 \leq \ell \leq t} \frac{\left|S_{h,-\ell}\right|}{h\ell} + \frac{5}{2} S_f + \frac{5}{2} S_g .$$

Proof: Observing that

$$\sin 2\pi hx \sin 2\pi \ell y = \frac{1}{2} \cos 2\pi(hx - \ell y) - \frac{1}{2} \cos 2\pi(hx + \ell y) , \tag{17}$$

one obtains from Lemma 3,

$$\rho(x)\rho(y) = \frac{1}{2\pi^2} \sum_{1 \leq h \leq t} \sum_{1 \leq \ell \leq t} \frac{\cos 2\pi(hx - \ell y)}{h\ell} - \frac{1}{2\pi^2} \sum_{1 \leq h \leq t} \sum_{1 \leq \ell \leq t} \frac{\cos 2\pi(hx + \ell y)}{h\ell} + \frac{5}{2}\eta\left[\min\left(1, \frac{1}{2\pi t\|x\|}\right) + \min\left(1, \frac{1}{2\pi t\|y\|}\right)\right] . \tag{18}$$

Replacing x by f(j), y by g(j), and summing with respect to j, Equation (18) yields

$$R = \frac{1}{2\pi^2} \sum_{1 \le h \le 1} \sum_{1 \le \ell \le t} \frac{1}{h\ell} \sum_{a < j \le b} \cos 2\pi(hf(j) - \ell g(j)) - \frac{1}{2\pi^2} \sum_{1 \le h \le t} \sum_{1 \le \ell \le t} \frac{1}{h\ell} \sum_{a < j \le b} \cos 2\pi(hf(j) + \ell g(j)) + \frac{5}{2} S_f + \frac{5}{2} S_g . \tag{19}$$

Thus

$$|R| < \frac{1}{2\pi^2} \sum_{1 \le h \le t} \sum_{1 \le \ell \le t} \frac{1}{h\ell} \left| \sum_{a < j \le b} \cos 2\pi(hf(j) - \ell g(j)) \right| + \frac{1}{2\pi^2} \sum_{1 \le h \le t} \sum_{1 \le \ell \le t} \frac{1}{h\ell} \left| \sum_{a < j \le b} \cos 2\pi(hf(j) + \ell g(j)) \right| + S_f + S_g . \tag{20}$$

Since

$$\left| \sum_{a \le j \le b} \cos 2\pi(hf(j) - \ell g(j)) \right| \le |S_{h,\ell}| ,$$

$$\left| \sum_{a < j \le b} \cos 2\pi(hf(j) + \ell g(j)) \right| \le |S_{h,\ell}| , \tag{21}$$

the lemma follows.

For the sequence given by

$$x_j = \left(\frac{a}{m} j^2\right), \quad (a,m) = 1 , \tag{22}$$

it is necessary to estimate

$$R = \sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2 - \alpha\right) \rho\left(\frac{a}{m}(j+\tau)^2 - \beta\right) , \tag{23}$$

in which α,β satisfy $0 \leq \alpha < 1$, $0 \leq \beta < 1$. Let

$$f(j) = \frac{a}{m} j^2 - \alpha , \tag{24}$$

$$g(j) = \frac{a}{m}(j+\tau)^2 - \beta ; \tag{25}$$

then,

Lemma 5:

$$\left|S_{h,\ell}\right| \leq \sqrt{2m(h+\ell,m)} .$$

Proof: One has

$$\left|S_{h,\ell}\right| = \left| \sum_{j=0}^{m-1} e\left(\frac{a}{m} hj^2 + \frac{a}{m} \ell(j+\tau)^2\right) \right| . \tag{26}$$

Let

$$\begin{aligned} d &= (h,\ell,m) , \\ h' &= h/d , \\ \ell' &= \ell/d , \\ m' &= m/d ; \end{aligned} \tag{27}$$

then

$$\left|S_{h,\ell}\right| = \left| \sum_{j=0}^{m-1} e\left(\frac{ah'}{m'} j^2 + \frac{a\ell'}{m'} (j+\tau)^2\right) \right| = d \left| \sum_{j=0}^{m'-1} e\left(\frac{ah'}{m'} j^2 + \frac{a\ell'}{m'} (j+\tau)^2\right) \right| . \tag{28}$$

Let

$$S' = \sum_{j=0}^{m'-1} e\left(\frac{ah'}{m'} j^2 + \frac{a\ell'}{m'} (j+\tau)^2\right) ; \tag{29}$$

then

$$|S'| = \left| \sum_{j=0}^{m'-1} e\left(\frac{a}{m'}(h' + \ell')j^2 + \frac{2a\ell'\tau}{m'} j\right) \right| . \tag{30}$$

One has

$$|S'|^2 = \sum_{k=0}^{m'-1} \sum_{j=0}^{m'-1} e\left(\frac{a}{m'}(h' + \ell')(j^2 - k^2) + \frac{2a\ell'\tau}{m'} (j-k)\right) , \tag{31}$$

and

$$|S'|^2 = \sum_{k=0}^{m'-1} \sum_{j=k}^{m'-1+k} e\left(\frac{a}{m'}(h' + \ell')(j^2 - k^2) + \frac{2a\ell'\tau}{m'} (j-k)\right) . \tag{32}$$

Let

$$j = k + \nu , \tag{33}$$

in which ν is a new summation variable; then

$$|S'|^2 = \sum_{\nu=0}^{m'-1} \sum_{k=0}^{m'-1} e\left(\frac{2a}{m'}(h' + \ell')\nu k\right) e\left(\frac{a}{m'}(h' + \ell')\nu^2 + \frac{2a\ell'\tau}{m'} \nu\right) , \tag{34}$$

and hence,

$$|S'|^2 \leq \sum_{\nu=0}^{m'-1} \left| \sum_{k=0}^{m_{-1}} e\left(\frac{2a}{m'}(h' + \ell')\nu k\right) \right| . \tag{35}$$

Let

$$\delta = (h' + \ell', m'), \quad b = \frac{h' + \ell'}{\delta}, \quad m'' = \frac{m'}{\delta} ; \tag{36}$$

then

$$\sum_{k=0}^{m'-1} e\left(\frac{2a}{m'}(h' + \ell')\nu k\right) = \sum_{k=0}^{m'-1} e\left(\frac{2ab}{m''} \nu k\right) = \delta \sum_{k=0}^{m''-1} e\left(\frac{2ab}{m''} \nu k\right) . \tag{37}$$

Thus, one obtains

$$|S'|^2 \leq \delta \sum_{\nu=0}^{m'-1} \left| \sum_{k=0}^{m'-1} e\left(\frac{2ab}{m''} \nu k\right) \right| . \tag{38}$$

By direct summation, one has

$$\begin{aligned} \sum_{k=0}^{m''-1} e\left(\frac{2ab}{m''} \nu k\right) &= 0, \quad m'' \nmid 2ab\nu \\ &= m'', \quad m'' \mid 2ab\nu . \end{aligned} \tag{39}$$

Since

$$(ab, m'') = 1 , \tag{40}$$

$m'' \mid 2ab\nu$ at most 2δ times, and hence,

$$|S'|^2 \leq 2\delta^2 m'' = 2\delta m' . \tag{41}$$

Equations (28), (29), and (41) now yield

$$\left|S_{h,\ell}\right| \leq d\sqrt{2\delta m'} = \sqrt{2\delta d^2 m'} = \sqrt{2\delta dm} = \sqrt{2m(h+\ell,m)} \; . \tag{42}$$

Lemma 5 yields a trivial estimate when applied to $S_{h,-h}$. It will be important to determine an accurate estimate for this quantity.

<u>Lemma 6</u>: $1 \leq \tau < \frac{m}{2t}$, $\nu \leq h \leq t$, $m > 2t$

$$\Longrightarrow \quad S_{h,-h} = 0 \; .$$

<u>Proof</u>: One has

$$\left|S_{h,-h}\right| = \left| \sum_{j=0}^{m-1} e\left(\frac{ah}{m}(j^2-(j+\tau)^2)\right)\right| = \left| \sum_{j=0}^{m-1} e\left(\frac{2ah\tau}{m}\, j\right)\right| \; . \tag{43}$$

Since $(a,m) = 1$, the sum in Equation (43) is zero when $m \nmid 2h\tau$. One has, for $1 \leq \tau < \frac{m}{2t}$, $1 \leq h \leq t$, $m > 2t$,

$$2 \leq 2h\tau \leq 2t\tau < m \; . \tag{44}$$

Thus, $m \mid 2h\tau$ and consequently, $S_{h,-h} = 0$.

<u>Lemma 7</u>: $t \geq 1$, $m > 2t$, $1 \leq \tau < \frac{m}{2t}$

$$\Longrightarrow |R| < \frac{\sqrt{m}}{\sqrt{2\pi^2}} \sum_{1 \leq h \leq t} \sum_{1 \leq \ell \leq t} \frac{1}{h\ell} \sqrt{(h+\ell,m)} +$$

$$\frac{\sqrt{m}}{\sqrt{2\pi^2}} \sum_{\substack{1 \leq h \leq t \\ h \neq \ell}} \sum_{1 \leq \ell \leq t} \frac{1}{h\ell} \sqrt{(h-\ell,m)} + \frac{5}{2} S_f + \frac{5}{2} S_g \; .$$

Proof: The lemma follows immediately from Lemmas 4, 5, and 6.

Lemma 8: For $t \geq 3$, one has

$$\frac{\sqrt{m}}{\sqrt{2\pi^2}} \sum_{1 \leq h \leq t} \sum_{1 \leq \ell \leq t} \frac{1}{h\ell} \sqrt{(h + \ell, m)} < \frac{\sqrt{m}}{\pi^2} (5.46 \ln^2 t + 3.27 \ln t \cdot \ln m)(2 + \sqrt{2})^{\nu(m)} ,$$

in which $\nu(m)$ denotes the number of distinct prime divisors of m.

Proof: In abbreviation, define S as follows.

$$S = \frac{\sqrt{m}}{\sqrt{2\pi^2}} \sum_{1 \leq h \leq t} \sum_{1 \leq \ell \leq t} \frac{1}{h\ell} \sqrt{(h + \ell, m)} . \tag{45}$$

Let h, ℓ be restricted so that $(h + \ell, m) = d$; then

$$S = \frac{\sqrt{m}}{\sqrt{2\pi^2}} \sum_{d \mid m} \sqrt{d} \sum_{\substack{1 \leq h \leq t \\ (h + \ell, m) = d}} \sum_{1 \leq \ell \leq t} \frac{1}{h\ell} . \tag{46}$$

The set of integers h, ℓ for which $(h + \ell, m) = d$ is included in the set for which $d \mid h + \ell$; hence

$$S \leq \frac{\sqrt{m}}{\sqrt{2\pi^2}} \sum_{d \mid m} \sqrt{d} \sum_{\substack{1 \leq h \leq t \\ d \mid h+\ell}} \sum_{1 \leq \ell \leq t} \frac{1}{h\ell} . \tag{47}$$

All integers fall into d residue classes modulo d. Let r denote the integers $0, 1, 2, \ldots, d-1$; then when h belongs to the residue class represented by r, ℓ

belongs to the class in which d-r is a member. Let S_r denote the following sum;

$$S_r = \sum_{\substack{1 \le h \le t \\ h=r(\mathrm{mod}\ d)}} \sum_{\substack{1 \le \ell \le t \\ \ell=d-r(\mathrm{mod}\ d)}} \frac{1}{h\ell} , \tag{48}$$

and S'(d) denote

$$S'(d) = \sum_{\substack{1 \le h \le t \\ d \mid h+\ell}} \sum_{1 \le \ell \le t} \frac{1}{h\ell} ; \tag{49}$$

then

$$S \le \frac{\sqrt{m}}{\sqrt{2\pi^2}} \sum_{d \mid m} \sqrt{d}\ S'(d) , \tag{50}$$

$$S'(d) = \sum_{r=0}^{d-1} S_r .$$

From the symmetry of the sum in Equation (48), it follows that

$$S_r = S_{d-r} , \tag{51}$$

and hence,

$$S'(d) = S_o + 2 \sum_{1 \le r \le d/2} S_r . \tag{52}$$

Setting $h = cd$ and $\ell = ed$ in which $c \geq 1$, $e \geq 1$ are new independent summation variables, one has

$$S_o = \frac{1}{d^2}\left(\sum_{1 \leq c \leq t/d} \frac{1}{c}\right)^2 \leq \frac{1}{d^2}\left(\sum_{1 \leq c \leq t} \frac{1}{c}\right)^2 . \tag{53}$$

Since, for $t \geq 3$,

$$\sum_{1 \leq c \leq t} \frac{1}{c} < 1 + \int_1^t \frac{dx}{x} = 1 + \ln t < 2 \ln t, \tag{54}$$

one obtains

$$S_o < \frac{4 \ln^2 t}{d^2} . \tag{55}$$

For r satisfying $1 \leq r \leq \frac{d}{2}$, let $h = cd + r$ and $\ell = ed - r$; then $h \geq 1$ implies $c \leq 0$, $\ell \geq 1$ implies $e \geq 1$, and

$$S_r \leq \sum_{0 \leq c \leq \frac{t-r}{d}} \frac{1}{cd+r} \cdot \sum_{1 \leq e \leq \frac{t+r}{d}} \frac{1}{ed-r} . \tag{56}$$

One has

$$\sum_{0 \leq c \leq \frac{t-r}{d}} \frac{1}{cd+r} \leq \frac{1}{r} + \int_o^{\frac{t-r}{d}} \frac{dx}{xd+r} = \frac{1}{r} + \frac{1}{d} \ln \frac{t}{r} \leq \frac{1}{r} + \frac{\ln t}{d} . \tag{57}$$

Also, one has

$$\sum_{1 \leq e \leq \frac{t+r}{d}} \frac{1}{ed+r} = \sum_{0 \leq e \leq \frac{t+r}{d} -1} \frac{1}{ed+d-r} \leq \frac{1}{d} \sum_{0 \leq e \leq \frac{t+r}{d} -1} \frac{1}{e+\frac{1}{2}} , \tag{58}$$

in which the inequality $r \leq \frac{d}{2}$ was used; further,

$$0 \leq e \leq \sum_{e+\frac{1}{2}}^{\frac{t+r}{d}-1} \frac{1}{e+\frac{1}{2}} \leq 2 + \int_{o}^{\frac{t+r}{d}-1} \frac{dx}{x+\frac{1}{2}} < 1.3 + \ln t < 2.3 \ln t. \quad (59)$$

Thus, one has

$$1 \leq \sum_{e \leq \frac{t+r}{d}} \frac{1}{ed+r} < \frac{2.3 \ln t}{d} . \quad (60)$$

Equations (56), (57), and (60) yield

$$S_r < \frac{2.3 \ln t}{rd} + \frac{2.3 \ln^2 t}{d^2} . \quad (61)$$

Equation (52) now takes the form

$$S'(d) < \frac{4 \ln^2 t}{d^2} + \frac{2.3 \ln^2 t}{d} + \frac{4.6 \ln t}{d} \sum_{1 \leq r \leq \frac{d}{2}} \frac{1}{r} . \quad (62)$$

Since

$$\frac{4 \ln^2 t}{d^2} \leq \frac{4 \ln^2 t}{d} , \quad (63)$$

and

$$1 \leq \sum_{r \leq \frac{d}{2}} \frac{1}{r} \leq 1 + \int_{1}^{\frac{d}{2}} \frac{dx}{x} = 1 + \ln \frac{d}{2} < .3 + \ln m , \quad (64)$$

in which the inequalities $\ln 2 < .7$ and $d \leq m$ were used, one obtains

$$S'(d) < \frac{7.68 \ln^2 t}{d} + \frac{4.6 \ln t \cdot \ln m}{d} . \tag{65}$$

Thus, Equation (50) yields

$$S < \frac{\sqrt{m}}{\sqrt{2\pi^2}} (7.68 \ln^2 t + 4.6 \ln t \cdot \ln m) \sum_{d|m} \frac{1}{\sqrt{d}} . \tag{66}$$

Let $\theta(a)$ be a multiplicative function of the integral variable a, and let

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_\nu^{\alpha_\nu} \tag{67}$$

be the canonical factorization of a; then the following identity holds[3]:

$$\sum_{d|a} \theta(d) = \prod_{p|a} [1 + \theta(p) + \theta(p^2) + \ldots + \theta(p^\alpha)] . \tag{68}$$

Employing Equation (68) with $\theta(d) = 1/\sqrt{d}$, a=m, one obtains

$$\sum_{d|m} \frac{1}{\sqrt{d}} = \prod_{p|m} [1 + \frac{1}{\sqrt{p}} + \frac{1}{(\sqrt{p})^2} + \ldots + \frac{1}{(\sqrt{p})^\alpha}] , \tag{69}$$

and hence,

$$\sum_{d|m} \frac{1}{\sqrt{d}} < \prod_{p|m} [1 + \frac{1}{\sqrt{p}} + \frac{1}{(\sqrt{p})^2} + \ldots] = \prod_{p|m} \frac{\sqrt{p}}{\sqrt{p} - 1} . \tag{70}$$

Since $p \geq 2$, one has $\sqrt{p}/(\sqrt{p} - 1) \leq 2 + \sqrt{2}$, and hence,

$$\sum_{d|m} \frac{1}{\sqrt{d}} \leq (2 + \sqrt{2})^{\nu(m)} . \tag{71}$$

Equations (66) and (71) now yield

$$S < \frac{\sqrt{m}}{\sqrt{2\pi^2}} (7.68 \ln^2 t + 4.6 \ln t \cdot \ln m)(2 + \sqrt{2})^{\nu(m)} . \tag{72}$$

Finally, use of the inequality $1/\sqrt{2} < .71$ yields the result of the lemma.

Lemma 9: For $t \geq 3$, one has

$$\frac{\sqrt{m}}{\sqrt{2\pi^2}} \sum_{\substack{1 \leq h \leq t \\ h \neq \ell}} \sum_{1 \leq \ell \leq t} \frac{1}{h\ell} \sqrt{(h - \ell, m)} < \frac{\sqrt{m}}{\pi^2} (8.52 \ln^2 t + 2.84 \ln t \cdot \ln m)(2 + \sqrt{2})^{\nu(m)} .$$

Proof: In abbreviation, define S by

$$S = \frac{\sqrt{m}}{\sqrt{2\pi^2}} \sum_{\substack{1 \leq h \leq t \\ h \neq \ell}} \sum_{1 \leq \ell \leq t} \frac{1}{h\ell} \sqrt{(h - \ell, m)} . \tag{73}$$

As in the proof of the preceding lemma, one may write

$$S = \frac{\sqrt{m}}{\sqrt{2\pi^2}} \sum_{d \mid m} \sqrt{d} \sum_{\substack{1 \leq h \leq t \\ (h - \ell, m) = d \\ h \neq \ell}} \sum_{1 \leq \ell \leq t} \frac{1}{h\ell} . \tag{74}$$

Define S'(d) by

$$S'(d) = \sum_{\substack{1 \leq h \leq t \\ d \mid h - \ell \\ h \neq \ell}} \sum_{1 \leq \ell \leq t} \frac{1}{h\ell} ; \tag{75}$$

then, since the class of integers satisfying $(h - \ell, m) = d$ is included in the class $d \mid h - \ell$, one has

$$S \leq \frac{\sqrt{m}}{\sqrt{2\pi^2}} \sum_{d \mid m} \sqrt{d}\, S'(d) \quad . \tag{76}$$

When h belongs to the residue class represented by r, then ℓ belongs to the same residue class. Let S_r denote the following sum:

$$S_r = \sum_{\substack{1 \leq h \leq t \\ h \equiv r \pmod d}} \sum_{\substack{1 \leq \ell \leq t \\ \ell \equiv r \pmod d \\ h \neq \ell}} \frac{1}{h\ell} \; ; \tag{77}$$

then

$$S'(d) = \sum_{r=0}^{d-1} S_r \; . \tag{78}$$

Setting $h = cd$, $\ell = ed$, the inequalities $1 \leq h \leq t$, $1 \leq \ell \leq t$ imply $1 \leq c \leq t/d$, $1 \leq e \leq t/d$, and

$$S_o \leq \frac{1}{d^2} \left(\sum_{1 \leq c \leq t/d} \frac{1}{c} \right)^2 < \frac{4 \ln^2 t}{d^2} \quad . \tag{79}$$

For $1 \leq r < d$, let $h = cd + r$, $\ell = ed + r$; then $1 \leq h \leq t$, $1 \leq \ell \leq t$ imply $0 \leq c \leq \frac{t-r}{d}$, $0 \leq e \leq \frac{t-r}{d}$, and

$$S_r = \sum_{\substack{0 \le c \le \frac{t-r}{d} \\ c \neq e}} \sum_{0 \le e \le \frac{t-r}{d}} \frac{1}{(cd+r)(ed+r)} . \tag{80}$$

Due to the symmetry of the sum in Equation (80),

$$S_r \le 2 \sum_{0 \le c \le \frac{t-r}{d}} \frac{1}{cd+r} \cdot \sum_{1 \le e \le \frac{t-r}{d}} \frac{1}{ed+r} . \tag{81}$$

Equation (57) yields

$$\sum_{0 \le c \le \frac{t-r}{d}} \frac{1}{cd+r} \le \frac{1}{r} + \frac{\ln t}{d} ; \tag{82}$$

further,

$$\sum_{1 \le e \le \frac{t-r}{d}} \frac{1}{ed+r} < \frac{1}{d} \sum_{1 \le e \le t} \frac{1}{e} < \frac{1}{d} (1 + \ln t) < \frac{2 \ln t}{d} , \tag{83}$$

and hence,

$$S_r < \frac{4 \ln t}{rd} \quad \frac{4 \ln^2 t}{d^2} . \tag{84}$$

Since $1 \le d \le m$ and

$$\sum_{r=1}^{d-1} \frac{1}{r} < 1 + \ln m , \tag{85}$$

Equations (78) and (84) yield

$$S'(d) < \frac{12 \ln^2 t}{d} + \frac{4 \ln t \cdot \ln m}{d} . \tag{86}$$

From Equations (76) and (86), one now has

$$S < \frac{\sqrt{m}}{\sqrt{2\pi^2}} (12 \ln^2 t + 4 \ln t \cdot \ln m) \sum_{d|m} \frac{1}{\sqrt{d}} . \tag{87}$$

Equation (71) and the inequality $1/\sqrt{2} < .71$ yield the result of the lemma.

Lemma 10: $(a,m) = 1$, $0 \leq \alpha < 1$, $0 \leq \beta < 1$, $m \geq 2\pi t$

$$\Longrightarrow \quad S_f < 3.2^{\nu(m)} \frac{m \ln m}{t} ,$$

$$S_g < 3.2^{\nu(m)} \frac{m \ln m}{t} .$$

Proof: Consider, in the sum

$$S_f = \sum_{j=0}^{m-1} \min \left(1, \frac{1}{\left\| \frac{a}{m} j^2 - \alpha \right\|}\right) , \tag{88}$$

regrouping the terms so that all j for which

$$aj^2 \equiv r \pmod{m}, \quad 0 \leq r < m \tag{89}$$

constitute the sum Σ_r; then

$$S_f = \sum_{r=0}^{m-1} \Sigma_r . \tag{90}$$

Let

$$m = 2^{\alpha} p_1^{\alpha_1} \cdots p_k^{\alpha_k} \tag{91}$$

be the canonical factorization of m; then, by a standard theorem,[3] the number of j for which $aj^2 \equiv r \pmod{m}$ is $T\,T_1 \cdots T_k$ where T_ℓ is the number of solutions of $aj^2 \equiv r \pmod{p_\ell^{\alpha_\ell}}$ and T is the number of solutions of $aj^2 \equiv r \pmod{2^\alpha}$. Also, one has[3]

$$T_\ell \leq 2, \quad 1 \leq \ell \leq k \tag{92}$$
$$T \leq 4 .$$

Hence,

$$T\,T_1 \cdots T_k \leq 4 \cdot 2^k \tag{93}$$

and, since $\nu(m) = k + 1$,

$$T\,T_1 \cdots T_k \leq 2 \cdot 2^{\nu(m)} . \tag{94}$$

Thus,

$$\Sigma_r \leq 2 \cdot 2^{\nu(m)} \min\left(1, \frac{1}{\|\frac{r}{m} - \alpha\|}\right) , \tag{95}$$

and hence,

$$S_f \leq 2 \cdot 2^{\nu(m)} \sum_{r=0}^{m-1} \min\left(1, \frac{1}{\|\frac{r}{m} - \alpha\|}\right) . \tag{96}$$

The sum in Equation (96) will be estimated by consideration of four cases.

Case 1: $-1 < \frac{r}{m} - \alpha \leq -\frac{1}{2}$.

One has

$$\|\tfrac{r}{m} - \alpha\| = 1 + \tfrac{r}{m} - \alpha , \tag{97}$$

and

$$0 \le \sum_{r \le m(\alpha-\frac{1}{2})} \min\left(1, \frac{1}{2\pi t(1 + \frac{r}{m} - \alpha)}\right) \le 1 + \int_0^{m(\alpha - \frac{1}{2})} \min\left(1, \frac{1}{2\pi t(1 + \frac{x}{m} - \alpha)}\right) dx,$$

$$< 1 + m\int_0^{\frac{1}{2}} \min\left(1, \frac{1}{2\pi tu}\right) du \,, \tag{98}$$

$$< 1 + \frac{m \ln \pi t}{\pi t} \,.$$

Case 2: $-\frac{1}{2} < \frac{r}{m} - \alpha \le 0$.

One has

$$\left\|\frac{r}{m} - \alpha\right\| = \alpha - \frac{r}{m} \,, \tag{99}$$

and

$$0 < \sum_{r \le m\alpha} \min\left(1, \frac{1}{2\pi t(\alpha - \frac{r}{m})}\right) \le 1 + \int_0^{m\alpha} \min\left(1, \frac{1}{2\pi t(\alpha - \frac{x}{m})}\right) dx \,,$$

$$< 1 + m\int_0^{1} \min\left(1, \frac{1}{2\pi tu}\right) du \,, \tag{100}$$

$$< 1 + \frac{m \ln 2\pi t}{\pi t} \,.$$

Case 3: $0 < \frac{r}{m} - \alpha \le \frac{1}{2}$.

One has

$$\left\|\frac{r}{m} - \alpha\right\| = \frac{r}{m} - \alpha \,, \tag{101}$$

and

$$m\alpha < \sum_{r} < m \quad \min\left(1, \frac{1}{2\pi t(\frac{r}{m} - \alpha)}\right) \leq 1 + \int_{m\alpha}^{m} \min\left(1, \frac{1}{2\pi t(\frac{x}{m} - \alpha)}\right) dx ,$$

$$< 1 + m \int_{o}^{1} \min\left(1, \frac{1}{2\pi tu}\right) du , \qquad (102)$$

$$< 1 + \frac{m \ln 2\pi t}{\pi t} .$$

Case 4: $\frac{1}{2} < \frac{r}{m} - \alpha < 1$.

One has

$$\left\| \frac{r}{m} - \alpha \right\| = 1 - \frac{r}{m} + \alpha , \qquad (103)$$

and

$$\sum_{m(\alpha + \frac{1}{2}) < r < m} \min\left(1, \frac{1}{2\pi t(1 - \frac{r}{m} + \alpha)}\right) \leq 1 +$$

$$\int_{m(\alpha + \frac{1}{2})}^{m} \min\left(1, \frac{1}{2\pi t(1 - \frac{x}{m} + \alpha)}\right) dx ,$$

$$\leq 1 + m \int_{o}^{\frac{1}{2}} \min\left(1, \frac{1}{2\pi tu}\right) du, \qquad (104)$$

$$< 1 + \frac{m \ln \pi t}{\pi t} .$$

One has

$$S_f < 2.2^{\nu(m)} \left[4 + \frac{2m \ln \pi t}{\pi t} + \frac{2m \ln 2\pi t}{\pi t}\right] , \qquad (105)$$

and

$$S_f < 8.2^{\nu(m)}\left[1 + \frac{m \ln 2\pi t}{\pi t}\right] . \tag{106}$$

Since $m \geq 2\pi t$, one has $\ln 2\pi t \leq \ln m$, and hence,

$$S_f < 8.2^{\nu(m)}\left[1 + \frac{m \ln m}{\pi t}\right] . \tag{107}$$

Also, since $m \ln m \geq 2\pi t$, one has

$$S_f < 12.2^{\nu(m)} \frac{m \ln m}{\pi t} . \tag{108}$$

Using the inequality $\pi > 3$ yields the result of the lemma. For the sum S_g, one has

$$S_g = \sum_{j=0}^{m-1} \min\left(1, \frac{1}{\left\|\frac{a}{m}(j+\tau)^2-\beta\right\|}\right) = \sum_{j=0}^{m-1} \min\left(1, \frac{1}{\left\|\frac{a}{m}\, j^2-\beta\right\|}\right) \tag{109}$$

and hence, the estimate obtained for S_f above applies also to S_g.

It is now possible to state the first main theorem.

THEOREM 1: $(a,m) = 1$, $m \geq 36$, $1 \leq \tau < \sqrt{m}$, $0 \leq \alpha < 1$, $0 \leq \beta < 1$,

$$\Longrightarrow \quad \left| \sum_{j=0}^{m-1} \rho\left(\frac{a}{m}\, j^2-\alpha\right)\rho\left(\frac{a}{m}(j+\tau)^2-\beta\right)\right| < \sqrt{m}\left[\frac{2}{3}\,(2+\sqrt{2})^{\nu(m)}\, \ln^2 m + 30.2^{\nu(m)}\, \ln m\right] .$$

Proof: Lemmas 7, 8, 9, and 10 yield

$$|R| < \frac{\sqrt{m}}{\pi^2}\left[13.98 \ln^2 t + 6.11 \ln t \cdot \ln m\right](2+\sqrt{2})^{\nu(m)} + 15.2^{\nu(m)} \frac{m \ln m}{t} . \tag{110}$$

Since $\pi^2 > 9.85$, one also has

$$|R| < \sqrt{m}\,[1.42\,\ln^2 t + .621\,\ln t \cdot \ln m](2+\sqrt{2})^{\nu(m)} + 15.2^{\nu(m)}\,\frac{m\ln m}{t}\,. \tag{111}$$

Choose

$$t = \frac{1}{2}\sqrt{m}\,; \tag{112}$$

then, since $\ln t < \frac{1}{2}\ln m$,

$$|R| < \sqrt{m}\,[\tfrac{2}{3}(2+\sqrt{2})^{\nu(m)}\,\ln^2 m + 30.2^{\nu(m)}\,\ln m]\,. \tag{113}$$

The conditions $t \geq 3$, $m \geq 2\pi t$ are both met by the condition $m \geq 36$. Since $m/2t = \sqrt{m}$, the condition $1 \leq \tau < m/2t$ becomes $1 \leq \tau < \sqrt{m}$. The theorem is now established.

The autocorrelation function of the sequence $x_j = \{\frac{a}{m} j^2\}$ is obtained immediately from Theorem 1 by setting $\alpha = 0$, $\beta = 0$, and recalling that $\psi(\tau) = R/m$. Hence, one has

THEOREM 2: $(a,m) = 1$, $m \geq 36$, $1 \leq \tau < \sqrt{m}$

$$\Longrightarrow\ |\psi(\tau)| < m^{-\frac{1}{2}}[\tfrac{2}{3}(2+\sqrt{2})^{\nu(m)}\,\ln^2 m + 30.2^{\nu(m)}\,\ln m]\,.$$

Consider the simultaneous Diophantine inequalities

$$0 \leq \{\tfrac{a}{m} j^2\} < \alpha,\ 0 \leq \{\tfrac{a}{m}(j+\tau)^2\} < \beta,\ 0 \leq j < m\,. \tag{114}$$

Let the number of solutions of the inequalities be designated by $T(\alpha,\beta)$, then

$$G(\alpha,\beta) = \frac{T(\alpha,\beta)}{m} \tag{115}$$

is the joint distribution function of the sequences $\{\frac{a}{m} j^2\}$, $\{\frac{a}{m}(j+\tau)^2\}$. If the sequences $\{\frac{a}{m} j^2\}$, $\{\frac{a}{m}(j+\tau)^2\}$ were independently equidistributed over (0,1), one would have $G(\alpha,\beta) = \alpha\beta$. It is the present object to determine the deviation of $G(\alpha,\beta)$ from the desired joint distribution $\alpha\beta$. For this purpose, let

$$H_\alpha(x) = \alpha + \rho(x) - \rho(x - \alpha) \; ; \tag{116}$$

then $H_\alpha(x)$ is a periodic function with period 1 and, within the initial period,

$$\begin{aligned} H_\alpha(x) &= 1, \quad 0 \le x < \alpha \, , \\ &= 0, \quad \alpha \le x < 1 \, . \end{aligned} \tag{117}$$

In view of the above properties of $H_\alpha(x)$, the enumeration $T(\alpha,\beta)$ is given by

$$T(\alpha,\beta) = \sum_{j=0}^{m-1} H_\alpha(\tfrac{a}{m} j^2) \; H_\beta(\tfrac{a}{m}(j+\tau)^2) \, . \tag{118}$$

<u>Lemma 11</u>: $T(\alpha,\beta) = \alpha\beta m + \beta \sum_{j=0}^{m-1} \rho(\frac{a}{m} j^2) - \beta \sum_{j=0}^{m-1} \rho(\frac{a}{m} j^2 - \alpha) +$

$$\alpha \sum_{j=0}^{m-1} \rho(\tfrac{a}{m}(j+\tau)^2) + \alpha \sum_{j=0}^{m-1} \rho(\tfrac{a}{m}(j+\tau)^2 - \beta) +$$

$$\sum_{j=0}^{m-1} \rho(\tfrac{a}{m} j^2) \, \rho(\tfrac{a}{m}(j+\tau)^2) - \sum_{j=0}^{m-1} \rho(\tfrac{a}{m} j^2 - \alpha) \, \rho(\tfrac{a}{m}(j+\tau)^2) -$$

$$\sum_{j=0}^{m-1} \rho(\tfrac{a}{m} j^2) \, \rho(\tfrac{a}{m}(j+\tau)^2 - \beta) + \sum_{j=0}^{m-1} \rho(\tfrac{a}{m} j^2 - \alpha) \, \rho(\tfrac{a}{m}(j+\tau)^2 - \beta) \, .$$

<u>Proof</u>: Use Equations (116) and (118).

Lemma 12: $(a,m) = 1$, $m \geq 36$, $1 \leq \tau < \sqrt{m}$, $0 \leq \alpha < 1$, $0 \leq \beta < 1$,

$$\Rightarrow \quad |T(\alpha,\beta) - \alpha\beta m| < 2 \left| \sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2\right) \right| + \left| \sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2 - \alpha\right) \right| + \left| \sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2 - \beta\right) \right| +$$

$$\sqrt{m}\left[\frac{8}{3} (2+\sqrt{2})^{\nu(m)} \ln^2 m + 120 \cdot 2^{\nu(m)} \ln m\right] .$$

Proof: Theorem 1 enables the estimation of the sums of products of the ρ-functions to be effected. Also observing that

$$\sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2\right) = \sum_{j=0}^{m-1} \rho\left(\frac{a}{m}(j+\tau)^2\right) , \tag{119}$$

$$\sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2 - \beta\right) = \sum_{j=0}^{m-1} \rho\left(\frac{a}{m}(j+\tau)^2 - \beta\right) , \tag{120}$$

the lemma follows.

In order to estimate the sum of the ρ-functions in Lemma 12, the following lemmas are required.

Lemma 13: $(a,m) = 1$, $0 \leq \alpha < 1$,

$$\Rightarrow \quad \left| \sum_{j=0}^{m-1} e\left(\frac{ha}{m} j^2 - h\alpha\right) \right| \leq \sqrt{2m(h,m)} .$$

Proof: Let

$$\begin{aligned} (h,m) &= d , \\ h' &= \frac{h}{d} , \\ m' &= \frac{m}{d} , \end{aligned} \tag{121}$$

and

$$S = \sum_{j=0}^{m-1} e\left(\frac{ha}{m} j^2 - h\alpha\right) ; \tag{122}$$

then

$$|S| = \left|\sum_{j=0}^{m-1} e\left(\frac{ha}{m} j^2\right)\right| = d \left|\sum_{j=0}^{m'-1} e\left(\frac{h'a}{m'} j^2\right)\right| . \tag{123}$$

One has

$$\begin{aligned} |S|^2 = d^2 \sum_{k=0}^{m'-1} \sum_{j=0}^{m'-1} e\left(\frac{h'a}{m'} j^2 - \frac{h'a}{m'} k^2\right) = \\ d^2 \sum_{k=0}^{m'-1} \sum_{j=k}^{m'-1+k} e\left(\frac{h'a}{m'} j^2 - \frac{h'a}{m'} k^2\right) . \end{aligned} \tag{124}$$

Introduce a new summation variable ν by

$$j = k+\nu ; \tag{125}$$

then

$$|S|^2 = d^2 \sum_{\nu=0}^{m'-1} \sum_{k=0}^{m'-1} e\left(\frac{2h'a}{m'}\nu k\right) e\left(\frac{h'a}{m'}\nu^2\right) \le d^2 \sum_{\nu=0}^{m'-1} \left| \sum_{k=0}^{m'-1} e\left(\frac{2h'a}{m'}\nu k\right)\right| . \tag{126}$$

By direct summation, one obtains

$$\begin{aligned} \sum_{k=0}^{m'-1} e\left(\frac{2h'a}{m'}\nu k\right) = 0, \quad m' \nmid 2h'a\nu , \\ = m', \quad m' \mid 2h'a\nu . \end{aligned} \tag{127}$$

Since $(h'a,m') = 1$, $m' \mid 2h'a\nu$ if and only if $m' \mid 2\nu$ which may occur at most twice. Hence,

$$|S|^2 \leq 2d^2m' = 2md \,. \tag{128}$$

The lemma follows on taking the square root.

Lemma 14: $(a,m) = 1,\ 0 \leq \alpha < 1,$

$$\Longrightarrow \left|\sum_{j=0}^{m-1}\rho\left(\frac{a}{m}\,j^2 - \alpha\right)\right| < \frac{\sqrt{2m}}{\pi} \sum_{1 \leq k \leq \frac{1}{2}\sqrt{m}} \frac{1}{h}\sqrt{(h,m)} + 6\sqrt{m}\,2^{\nu(m)} \ln m \,.$$

Proof: Use of Lemma 1 yields

$$\left|\sum_{j=0}^{m-1}\rho\left(\frac{a}{m}\,j^2 - \alpha\right)\right| < \sum_{1 \leq h \leq t} \frac{1}{\pi h}\left|\sum_{j=0}^{m-1} e\left(\frac{ha}{m}\,j^2\right)\right| + \sum_{j=0}^{m-1} \min\left(1, \frac{1}{2\pi t\left\|\frac{a}{m}\,j^2 - \alpha\right\|}\right) . \tag{129}$$

Setting $t = \frac{1}{2}\sqrt{m}$ and using Lemma 9, one obtains

$$\left|\sum_{j=0}^{m-1}\rho\left(\frac{a}{m}\,j^2 - \alpha\right)\right| < \sum_{1 \leq h \leq \frac{1}{2}\sqrt{m}} \frac{1}{\pi h}\left|\sum_{j=0}^{m-1} e\left(\frac{ha}{m}\,j^2\right)\right| + 6\sqrt{m}2^{\nu(m)} \ln m. \tag{130}$$

The lemma now follows on employing Lemma 13.

Lemma 15: $(a,m) = 1,\ 0 \leq \alpha < 1,\ m \geq 36$

$$\Longrightarrow \left|\sum_{j=0}^{m-1}\rho\left(\frac{a}{m}\,j^2 - \alpha\right)\right| < 3.92\sqrt{m}\,(2+\sqrt{2})^{\nu(m)} \ln m \,.$$

Proof: One has

$$\frac{\sqrt{2m}}{\pi} \sum_{1 \le h \le \frac{1}{2}\sqrt{m}} \frac{1}{h}\sqrt{(h,m)} = \frac{\sqrt{2m}}{\pi} \sum_{d|m} \sqrt{d} \sum_{\substack{1 \le h \le \frac{1}{2}\sqrt{m} \\ (h,m) = d}} \frac{1}{h} \le \tag{131}$$

$$\frac{\sqrt{2m}}{\pi} \sum_{d|m} \sqrt{d} \sum_{\substack{1 \le h \le \frac{1}{2}\sqrt{m} \\ d|h}} \frac{1}{h} .$$

Let $h = cd$; then

$$\frac{\sqrt{2m}}{\pi} \sum_{d|m} \sqrt{d} \sum_{\substack{1 \le h \le \frac{1}{2}\sqrt{m} \\ d|h}} \frac{1}{h} < \frac{\sqrt{2m}}{\pi} \sum_{d|m} \frac{1}{\sqrt{d}} \sum_{1 \le c \le \frac{1}{2}\sqrt{m}} \frac{1}{c} < \tag{132}$$

$$\sqrt{m}(.15 + .27 \ln m) \sum_{d|m} \frac{1}{\sqrt{d}} .$$

Use of Equation (71) now yields

$$\frac{\sqrt{2m}}{\pi} \sum_{1 \le h \le \frac{1}{2}\sqrt{m}} \frac{1}{h}\sqrt{(h,m)} < \sqrt{m}(.15 + .27 \ln m)(2 + \sqrt{2})^{\nu(m)} . \tag{133}$$

Since $m \ge 36$, one has

$$.15 + .27 \ln m < .312 \ln m , \tag{134}$$

and hence,

$$\frac{\sqrt{2m}}{\pi} \sum_{1 \le h \le \frac{1}{2}\sqrt{m}} \frac{1}{h}\sqrt{(h,m)} < .312 \sqrt{m} (2 + \sqrt{2})^{\nu(m)} \ln m . \tag{135}$$

Lemma 14 now yields

$$\left|\sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2 - \alpha\right)\right| < .312\sqrt{m}\,(2+\sqrt{2})^{\nu(m)} \ln m + 6\sqrt{m}\,2^{\nu(m)} \ln m . \quad (136)$$

Since $2/(2+\sqrt{2}) < 1$ and $\nu(m) \geq 1$, one has

$$.312\,(2+\sqrt{2})^{\nu(m)} + 6.2^{\nu(m)} \leq 3.92\,(2+\sqrt{2})^{\nu(m)} . \quad (137)$$

This proves the lemma.

THEOREM 3: $(a,m) = 1$, $m \geq 36$, $1 \leq \tau < \sqrt{m}$,

$$\Longrightarrow \left|G(\alpha,\beta) - \alpha\beta\right| < m^{-\frac{1}{2}}\,(2+\sqrt{2})^{\nu(m)}\left(\frac{8}{3}\ln^2 m + 88 \ln m\right) .$$

Proof: Lemmas 12, and 15 provide the following inequality.

$$\left|G(\alpha,\beta) - \alpha\beta\right| < m^{-\frac{1}{2}}\left[\frac{8}{3}\,(2+\sqrt{2})^{\nu(m)} \ln^2 m + \left(15.68(2+\sqrt{2})^{\nu(m)} + 120.2^{\nu(m)}\right) \ln m\right] . \quad (138)$$

Using the inequality

$$2^{\nu(m)} < .6(2+\sqrt{2})^{\nu(m)} , \quad (139)$$

The theorem follows.

Theorem 3 thus demonstrates that the sequences $\{\frac{a}{m} j^2\}$, $\{\frac{a}{m}(j+\tau)^2\}$ are approximately independently equidistributed over (0,1).

References

1. Hardy, G. H. Divergent Series. Oxford: Clarendon Press, 1949.

2. Franklin, J. N. Deterministic Simulation of Random Processes. Technical Report No. 118, January, 1962. California Institute of Technology.

3. Vinogradov, I. M. Elements of Number Theory. New York: Dover Publications, 1954.

UNCLASSIFIED

System Development Corporation,
Santa Monica, California
THE AUTOCORRELATION AND JOINT
DISTRIBUTION FUNCTIONS OF THE
SEQUENCES, $\{\frac{a}{m} j^2\}$, $\{\frac{a}{m}(j/\tau)^2\}$

Scientific rept., TM-1042/203/00,
by D. L. Jagerman, 15 March 1963,
34p., 3 refs.

Unclassified report

DESCRIPTORS: Monte Carlo Method.

States that the present-day
extensive use of Monte Carlo UNCLASSIFIED

---

procedures necessitates the UNCLASSIFIED
careful investigation of methods
for the generation of random numbers.
Also states that in its simplest form,
the underlying principle of all Monte
Carlo procedures finds its expression
in the following theorem:
Let $(x_j)_1^\infty$ be a sequence equidistributed
over (0,1), and let f(x) be a function
Riemann integrable on (0,1); then

$\sum_{j=1}^{N} f(x_j) \sim N \int_0^1 f(x)dx.$ UNCLASSIFIED