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

By David 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 many 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 characteristics. 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

$$x = \left(\left\{\frac{a}{m}j^2\right\}\right)_0^{m-1}, \qquad x^{(\tau)} = \left(\left\{\frac{a}{m}(j+\tau)^2\right\}\right)_0^{m-1}.$$

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

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

Received March 1, 1963, revised September 5, 1963.

For the sequence to be studied, this takes the form

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

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

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

the autocorrelation function is small; that is, quantitatively

$$|\psi(\tau)| < m^{-1/2}[.81(2+\sqrt{2})^{\nu(m)} \ln^2 m + 33(4+2\sqrt{2})^{\nu(m)} \ln m],$$

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

Let $H_\alpha(x)$ be given by $H_\alpha(x) = \alpha + \rho(x) - \rho(x-\alpha)$, that is, in the initial period,

$$\begin{aligned} H_\alpha(x) &= 1, & 0 \leqq x < \alpha, \\ &= 0, & \alpha \leqq x < 1, \end{aligned}$$

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

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

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

$$|G(\alpha, \beta) - \alpha\beta| < m^{-1/2}[3.24(2+\sqrt{2})^{\nu(m)} \ln^2 m + 392(4+2\sqrt{2})^{\nu(m)} \ln m].$$

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

The above enumerated properties show the possible applicability of the sequences $\left(\left\{\frac{a}{m}j^2\right\}\right)_0^{m-1}$, $\left(\left\{\frac{a}{m}(j+\tau)^2\right\}\right)_0^{m-1}$ 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. $t \geqq 1$

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

where

$$|\eta| < 1$$

and 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

$$\rho(x) = \sum_{h=1}^{\infty} \frac{\sin 2\pi hx}{\pi h} \tag{2.1}$$

hence, it is necessary to establish

$$\left| \sum_{h>t} \frac{\sin 2\pi hx}{\pi h} \right| < \min\left(1, \frac{1}{2\pi t \| x \|}\right). \tag{2.2}$$

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

$$\begin{aligned} &a_l \downarrow \geqq 0, \qquad \left| \sum_{p=M}^{l} b_p \right| \leqq B \\ &\Rightarrow \left| \sum_{l=M}^{\infty} a_l b_l \right| \leqq a_M B. \end{aligned} \tag{2.3}$$

Also standard is the following estimate:

$$\left| \sum_{p=M}^{l} \sin 2\pi px \right| \leqq \frac{1}{2 \| x \|}. \tag{2.4}$$

Applying the inequalities of Equations (2.3) and (2.4), one has

$$\left| \sum_{h>t} \frac{\sin 2\pi hx}{\pi h} \right| \leqq \frac{1}{2\pi([t] + 1)\| x \|} < \frac{1}{2\pi t \| x \|}. \tag{2.5}$$

If $2\pi t \| x \| > 1$, then Equation (2.2) has been established. Consider now the case $2\pi t \| x \| \leqq 1$, then

$$\sum_{h>t} \frac{\sin 2\pi hx}{\pi h} = \sum_{h=1}^{\infty} \frac{\sin 2\pi hx}{\pi h} - \sum_{1 \leqq h \leqq t} \frac{\sin 2\pi hx}{\pi h}. \tag{2.6}$$

Thus

$$\begin{aligned} \left| \sum_{h>t} \frac{\sin 2\pi hx}{\pi h} \right| &\leqq \frac{1}{2} + \left| \sum_{1 \leqq h \leqq t} \frac{\sin 2\pi hx}{\pi h} \right| \leqq \frac{1}{2} + \sum_{1 \leqq h \leqq t} \frac{|\sin 2\pi h \| x \| |}{\pi h} \\ &\leqq \frac{1}{2} + 2 \| x \| t \leqq \frac{1}{2} + \frac{1}{\pi} < 1. \end{aligned} \tag{2.7}$$

Equation (2.2) 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. $\left| \sum_{1 \leqq h \leqq t} \frac{\sin 2\pi hx}{\pi h} \right| < \frac{3}{2}.$

Proof. One has

$$\sum_{1\leqq h\leqq t}\frac{\sin 2\pi hx}{\pi h}=\sum_{h=1}^{\infty}\frac{\sin 2\pi hx}{\pi h}-\sum_{h>t}\frac{\sin 2\pi hx}{\pi h}. \tag{2.8}$$

Hence

$$\left|\sum_{1\leqq h\leqq t}\frac{\sin 2\pi hx}{\pi h}\right|\leqq\frac{1}{2}+\left|\sum_{h>t}\frac{\sin 2\pi hx}{\pi h}\right|<\frac{3}{2}. \tag{2.9}$$

The inequality of Lemma 1 was used.

LEMMA 3. $t\geqq 1$

$$\Rightarrow \rho(x)\rho(y)=\sum_{1\leqq h\leqq t}\sum_{1\leqq l\leqq t}\frac{\sin 2\pi hx\cdot\sin 2\pi ly}{\pi^2 hl}+\frac{5}{2}\eta\left[\min\left(1,\frac{1}{2\pi t\,\|x\|}\right)+\min\left(1,\frac{1}{2\pi t\,\|y\|}\right)\right],$$

where

$$|\eta|<1.$$

Proof. Use of Lemma 1 yields

$$\begin{aligned}\rho(x)\rho(y)&=\sum_{1\leqq h\leqq t}\sum_{1\leqq l\leqq t}\frac{\sin 2\pi hx\cdot\sin 2\pi ly}{\pi^2 hl}\\&+\eta\sum_{1\leqq h\leqq t}\frac{\sin 2\pi hx}{\pi h}\cdot\min\left(1,\frac{1}{2\pi t\,\|y\|}\right)+\eta\sum_{1\leqq l\leqq t}\frac{\sin 2\pi ly}{\pi l}\\&\cdot\min\left(1,\frac{1}{2\pi t\,\|x\|}\right)+\eta^2\min\left(1,\frac{1}{2\pi t\,\|x\|}\right)\min\left(1,\frac{1}{2\pi t\,\|y\|}\right).\end{aligned} \tag{2.10}$$

Lemma 2 allows one to write

$$\begin{aligned}\rho(x)\rho(y)&=\sum_{1\leqq h\leqq t}\sum_{1\leqq l\leqq t}\frac{\sin 2\pi hx\cdot\sin 2\pi ly}{\pi^2 hl}\\&+\frac{3}{2}\eta\left[\min\left(1,\frac{1}{2\pi t\,\|x\|}\right)+\min\left(1,\frac{1}{2\pi t\,\|y\|}\right)\right]\\&+\eta^2\min\left(1,\frac{1}{2\pi t\,\|x\|}\right)\min\left(1,\frac{1}{2\pi t\,\|y\|}\right).\end{aligned} \tag{2.11}$$

Observing that

$$\begin{aligned}\min\left(1,\frac{1}{2\pi t\,\|x\|}\right)\min\left(1,\frac{1}{2\pi t\,\|y\|}\right)&\leqq\min\left(1,\frac{1}{2\pi t\,\|x\|}\right)\\&\leqq\min\left(1,\frac{1}{2\pi t\,\|x\|}\right)+\min\left(1,\frac{1}{2\pi t\,\|y\|}\right),\end{aligned} \tag{2.12}$$

the lemma follows.

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

$$e(x)=e^{i2\pi x}, \tag{2.13}$$

R by

$$R = \sum_{a<j\leqq b} \rho(f(j))\rho(g(j)), \tag{2.14}$$

$S_{h,l}$ by

$$S_{h,l} = \sum_{a<j\leqq b} e(hf(j) + lg(j)), \tag{2.15}$$

and S_f by

$$S_f = \sum_{a<j\leqq b} \min\left(1, \frac{1}{2\pi t \| f(j) \|}\right), \tag{2.16}$$

then

LEMMA 4. $t \geqq 1$

$$\Rightarrow |R| < \frac{1}{2\pi^2} \sum_{1\leqq h\leqq t} \sum_{1\leqq l\leqq t} \frac{S_{h,l}}{hl} + \frac{1}{2\pi^2} \sum_{1\leqq h\leqq t} \sum_{1\leqq l\leqq t} \frac{S_{h,-l}}{hl} + \frac{5}{2} S_f + \frac{5}{2} S_g .$$

Proof. Observing that

$$\sin 2\pi hx \sin 2\pi ly = \tfrac{1}{2} \cos 2\pi(hx - ly) - \tfrac{1}{2} \cos 2\pi(hx + ly), \tag{2.17}$$

one obtains from Lemma 3

$$\begin{aligned} \rho(x)\rho(y) = {} & \frac{1}{2\pi^2} \sum_{1\leqq h\leqq t} \sum_{1\leqq l\leqq t} \frac{\cos 2\pi(hx - ly)}{hl} - \frac{1}{2\pi^2} \sum_{1\leqq h\leqq t} \sum_{1\leqq l\leqq t} \\ & \frac{\cos 2\pi(hx + ly)}{hl} + \frac{5}{2}\eta\left[\min\left(1, \frac{1}{2\pi t \| x \|}\right) + \min\left(1, \frac{1}{2\pi t \| y \|}\right)\right]. \end{aligned} \tag{2.18}$$

Replacing x by $f(j)$, y by $g(j)$, and summing with respect to j, Equation 2.18 yields

$$\begin{aligned} R = {} & \frac{1}{2\pi^2} \sum_{1\leqq h\leqq t} \sum_{1\leqq l\leqq t} \frac{1}{hl} \sum_{a<j\leqq b} \cos 2\pi(hf(j) - lg(j)) \\ & - \frac{1}{2\pi^2} \sum_{1\leqq h\leqq t} \sum_{1\leqq l\leqq t} \frac{1}{hl} \sum_{a<j\leqq b} \cos 2\pi(hf(j) + lg(j)) + \frac{5}{2}\eta(S_f + S_g). \end{aligned} \tag{2.19}$$

Thus

$$\begin{aligned} |R| < {} & \frac{1}{2\pi^2} \sum_{1\leqq h\leqq t} \sum_{1\leqq l\leqq t} \frac{1}{hl} \left| \sum_{a<j\leqq b} \cos 2\pi(hf(j) - lg(j)) \right| \\ & + \frac{1}{2\pi^2} \sum_{1\leqq h\leqq t} \sum_{1\leqq l\leqq t} \frac{1}{hl} \left| \sum_{a<j\leqq b} \cos 2\pi(hf(j) + lg(j)) \right| + \frac{5}{2} S_f + \frac{5}{2} S_g . \end{aligned} \tag{2.20}$$

Since

$$\begin{aligned} & \left| \sum_{a<j\leqq b} \cos 2\pi(hf(j) - lg(j)) \right| \leqq |S_{h,-l}|, \\ & \left| \sum_{a<j\leqq b} \cos 2\pi(hf(j) + lg(j)) \right| \leqq |S_{h,l}|, \end{aligned} \tag{2.21}$$

the lemma follows.

For the sequence given by

$$x_j = \left\{\frac{a}{m} j^2\right\}, \qquad (a, m) = 1, \tag{2.22}$$

it is necessary to estimate

$$R = \sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2 - \alpha\right) \rho\left(\frac{a}{m}(j+\tau)^2 - \beta\right), \tag{2.23}$$

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

$$f(j) = \frac{a}{m} j^2 - \alpha, \tag{2.24}$$

$$g(j) = \frac{a}{m}(j+\tau)^2 - \beta, \tag{2.25}$$

then,

LEMMA 5. $(a, m) = 1$,

$$\Rightarrow |S_{h,l}| \leqq \sqrt{2m(h+l, m)}$$

Proof. One has

$$|S_{h,l}| = \left|\sum_{j=0}^{m-1} e\left(\frac{a}{m} hj^2 + \frac{a}{m} l(j+\tau)^2\right)\right| \tag{2.26}$$

Let

$$\begin{aligned} d &= (h, l, m), \\ h' &= h/d, \\ l' &= l/d, \\ m' &= m/d, \end{aligned} \tag{2.27}$$

then

$$\begin{aligned} |S_{h,l}| &= \left|\sum_{j=0}^{m-1} e\left(\frac{ah'}{m'} j^2 + \frac{al'}{m'}(j+\tau)^2\right)\right| \\ &= d\left|\sum_{j=0}^{m'-1} e\left(\frac{ah'}{m'} j^2 + \frac{al'}{m'}(j+\tau)^2\right)\right|. \end{aligned} \tag{2.28}$$

Let

$$S' = \sum_{j=0}^{m'-1} e\left(\frac{ah'}{m'} j^2 + \frac{al'}{m'}(j+\tau)^2\right), \tag{2.29}$$

then

$$|S'| = \left|\sum_{j=0}^{m'-1} e\left(\frac{a}{m'}(h'+l')j^2 + \frac{2al'\tau}{m'} j\right)\right|. \tag{2.30}$$

One has

$$|S'|^2 = \sum_{k=0}^{m-1} \sum_{j=0}^{m'-1} e\left(\frac{a}{m'}(h'+l')(j^2-k^2) + \frac{2al'\tau}{m'}(j-k)\right), \tag{2.31}$$

and

$$|S'|^2 = \sum_{k=0}^{m'-1} \sum_{j=k}^{m'-1+k} e\left(\frac{a}{m'}(h'+l')(j^2-k^2) + \frac{2al'\tau}{m'}(j-k)\right). \tag{2.32}$$

Let

$$j = k + \nu, \tag{2.33}$$

in which ν is a new summation variable, then

$$|S'|^2 = \sum_{\nu=0}^{m'-1} \sum_{k=0}^{m'-1} e\left(\frac{2a}{m'}(h'+l')\nu k\right) e\left(\frac{a}{m'}(h'+l')\nu^2 + \frac{2al'\tau}{m'}\nu\right), \tag{2.34}$$

and hence,

$$|S'|^2 \leqq \sum_{\nu=0}^{m'-1} \left| \sum_{k=0}^{m'-1} e\left(\frac{2a}{m'}(h'+l')\nu k\right)\right|. \tag{2.35}$$

Let

$$\delta = (h'+l', m'), \qquad b = \frac{h'+l'}{\delta}, \qquad m'' = \frac{m'}{\delta}, \tag{2.36}$$

then

$$\sum_{k=0}^{m'-1} e\left(\frac{2a}{m'}(h'+l')\nu k\right) = \sum_{k=0}^{m'-1} e\left(\frac{2ab}{m''}\nu k\right) = \delta \sum_{k=0}^{m''-1} e\left(\frac{2ab}{m''}\nu k\right). \tag{2.37}$$

Thus one obtains

$$|S'|^2 \leqq \delta \sum_{\nu=0}^{m'-1} \left| \sum_{k=0}^{m''-1} e\left(\frac{2ab}{m''}\nu k\right)\right|. \tag{2.38}$$

By direct summation, one has

$$\sum_{k=0}^{m''-1} e\left(\frac{2ab}{m''}\nu k\right) = \begin{cases} 0, & m'' \nmid 2ab\nu \\ m'', & m'' \mid 2ab\nu. \end{cases} \tag{2.39}$$

Since

$$(ab, m'') = 1, \tag{2.40}$$

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

$$|S'|^2 \leqq 2\delta^2 m'' = 2\delta m'. \tag{2.41}$$

Equations (2.28), (2.29), and (2.41) now yield

$$|S_{h,l}| \leqq d\sqrt{2\delta m'} = \sqrt{2\delta d^2 m'} = \sqrt{2\delta d m} = \sqrt{2m(h+l, m)}. \tag{2.42}$$

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

LEMMA 6. $1 \leqq \tau < \dfrac{m}{2t}$, $1 \leqq h \leqq t$, $m > 2t$

$$\Rightarrow S_{h,-h} = 0.$$

Proof. One has

$$|S_{h,-h}| = \left|\sum_{j=0}^{m-1} e\left(\frac{ah}{m}(j^2-(j+\tau)^2)\right)\right| = \left|\sum_{j=0}^{m-1} e\left(\frac{2ah\tau}{m}j\right)\right|. \tag{2.43}$$

Since $(a, m) = 1$, the sum in Equation 2.43 is zero when $m \nmid 2h\tau$. One has, for $1 \leqq \tau < \frac{m}{2t}$, $1 \leqq h \leqq t$, $m > 2t$,

$$2 \leqq 2h\tau \leqq 2t\tau < m. \tag{2.44}$$

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

LEMMA 7. $t \geqq 1$, $m > 2t$, $1 \leqq \tau < \frac{m}{2t}$

$$\Rightarrow |R| < \frac{\sqrt{m}}{\sqrt{2}\pi^2} \sum_{1\leqq h\leqq t} \sum_{1\leqq l\leqq t} \frac{1}{hl}\sqrt{(h+l, m)} + \frac{\sqrt{m}}{\sqrt{2}\pi^2} \sum_{\substack{1\leqq h\leqq t \\ h\neq l}} \sum_{1\leqq l\leqq t} \frac{1}{hl}\sqrt{(h-l, m)} + \frac{5}{2}S_f + \frac{5}{2}S_g.$$

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

LEMMA 8. *For $t \geqq 3$, one has*

$$\frac{\sqrt{m}}{\sqrt{2}\pi^2} \sum_{1\leqq h\leqq t} \sum_{1\leqq l\leqq t} \frac{1}{hl}\sqrt{(h+l, m)} < \frac{\sqrt{m}}{\pi^2}(7.10\ln^2 t + 5.26\ln t\cdot\ln m)(2+\sqrt{2})^{\nu(m)},$$

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

Proof. In abbreviation, define S as follows.

$$S = \frac{\sqrt{m}}{\sqrt{2}\pi^2} \sum_{1\leqq h\leqq t} \sum_{1\leqq l\leqq t} \frac{1}{hl}\sqrt{(h+l, m)}. \tag{2.45}$$

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

$$S = \frac{\sqrt{m}}{\sqrt{2}\pi^2} \sum_{d\mid m} \sqrt{d} \sum_{\substack{1\leqq h\leqq t \\ (h+l,m)=d}} \sum_{1\leqq l\leqq t} \frac{1}{hl}. \tag{2.46}$$

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

$$S \leqq \frac{\sqrt{m}}{\sqrt{2}\pi^2} \sum_{d\mid m} \sqrt{d} \sum_{\substack{1\leqq h\leqq t \\ d\mid h+l}} \sum_{1\leqq l\leqq t} \frac{1}{hl}. \tag{2.47}$$

All integers fall into d residue classes modulo d. If r denotes one of the integers, 0, 1, 2, $\cdots$, $d - 1$, then when h belongs to the residue class represented by r, l belongs to the class in which $d - r$ is member. Let S_r denote the following sum

$$S_r = \sum_{\substack{1\leqq h\leqq t \\ h\equiv r(\mathrm{mod}\, d)}} \sum_{\substack{1\leqq l\leqq t \\ l\equiv d-r(\mathrm{mod}\, d)}} \frac{1}{hl} \tag{2.48}$$

and $S'(d)$ denote

$$S'(d) = \sum_{\substack{1 \leqq h \leqq t \\ d \mid h+l}} \sum_{1 \leqq l \leqq t} \frac{1}{hl}, \tag{2.49}$$

then

$$\begin{aligned} S &\leqq \frac{\sqrt{m}}{\sqrt{2\pi}^2} \sum_{d \mid m} \sqrt{d} S'(d), \\ S'(d) &= \sum_{r=0}^{d-1} S_r . \end{aligned} \tag{2.50}$$

From the symmetry of the sum in Equation (2.48), it follows that

$$S_r = S_{d-r} , \tag{2.51}$$

and hence

$$S'(d) \leqq S_0 + 2 \sum_{1 \leqq r \leqq d/2} S_r . \tag{2.52}$$

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

$$S_0 = \frac{1}{d^2} \left(\sum_{1 \leqq c \leqq t/d} \frac{1}{c} \right)^2 \leqq \frac{1}{d^2} \left(\sum_{1 \leqq c \leqq t} \frac{1}{c} \right)^2 . \tag{2.53}$$

Since, for $t \geqq 3$,

$$\sum_{1 \leqq c \leqq t} \frac{1}{c} < 1 + \int_1^t \frac{dx}{x} = 1 + \ln t < 2 \ln t, \tag{2.54}$$

one obtains

$$S_0 < \frac{4 \ln^2 t}{d^2} . \tag{2.55}$$

For r satisfying $1 \leqq r \leqq \frac{d}{2}$, let $h = cd + r$ and $l = ed - r$, then $h \geqq 1$ implies $c \geqq 0$, $l \geqq 1$ implies $e \geqq 1$, and

$$S_r \leqq \sum_{0 \leqq c \leqq \frac{t-r}{d}} \frac{1}{cd + r} \cdot \sum_{1 \leqq e \leqq \frac{t+r}{d}} \frac{1}{ed - r} . \tag{2.56}$$

One has

$$\sum_{0 \leqq c \leqq \frac{t-r}{d}} \frac{1}{cd + r} < \frac{1}{r} + \int_0^{\frac{t-r}{d}} \frac{dx}{xd + r} = \frac{1}{r} + \frac{1}{d} \ln \frac{t}{r} \leqq \frac{1}{r} + \frac{\ln t}{d} . \tag{2.57}$$

Also, one has

$$\sum_{1 \leqq e \leqq \frac{t+r}{d}} \frac{1}{ed - r} = \sum_{0 \leqq e \leqq \frac{t+r}{d} - 1} \frac{1}{ed + d - r} \leqq \frac{1}{d} \sum_{0 \leqq e \leqq \frac{t+r}{d} - 1} \frac{1}{e + \frac{1}{2}} , \tag{2.58}$$

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

$$\sum_{0 \leqq e \leqq \frac{t+r}{d}-1} \frac{1}{e+\frac{1}{2}} \leqq 2 + \int_0^{\frac{t+r}{d}-1} \frac{dx}{x+\frac{1}{2}} < 2.7 + \ln t < 3.7 \ln t. \tag{2.59}$$

Thus, one has

$$\sum_{1 \leqq e \leqq \frac{t+r}{d}} \frac{1}{ed-r} < \frac{3.7 \ln t}{d} \tag{2.60}$$

Equations 2.56, 2.57, and 2.60 yield

$$S_r < \frac{3.7 \ln t}{rd} + \frac{3.7 \ln^2 t}{d^2}. \tag{2.61}$$

Equation 2.52 now takes the form

$$S'(d) < \frac{4 \ln^2 t}{d^2} + \frac{3.7 \ln^2 t}{d} + \frac{7.4 \ln t}{d} \sum_{1 \leqq r \leqq \frac{d}{2}} \frac{1}{r}. \tag{2.62}$$

Since

$$\frac{4 \ln^2 t}{d^2} \leqq \frac{4 \ln^2 t}{d}, \tag{2.63}$$

and

$$\sum_{1 \leqq r \leqq \frac{d}{2}} \frac{1}{r} \leqq 1 + \int_1^{\frac{d}{2}} \frac{dx}{x} = 1 + \ln \frac{d}{2} < .31 + \ln m, \tag{2.64}$$

in which the inequalities $\ln 2 > .69$ and $d \leqq m$ were used, one obtains

$$S'(d) < \frac{10 \ln^2 t}{d} + \frac{7.4 \ln t \cdot \ln m}{d}. \tag{2.65}$$

Thus, Equation (2.50) yields

$$S < \frac{\sqrt{m}}{\sqrt{2\pi}^2} (10 \ln^2 t + 7.4 \ln t \cdot \ln m) \sum_{d \mid m} \frac{1}{\sqrt{d}}. \tag{2.66}$$

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

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_\nu^{\alpha_\nu} \tag{2.67}$$

be the canonical factorization of a, then the following identity holds [3].

$$\sum_{d \mid a} \theta(d) = \prod_{p \mid a} [1 + \theta(p) + \theta(p^2) + \cdots + \theta(p^\alpha)]. \tag{2.68}$$

Employing Equation (2.68) with $\theta(d) = 1/\sqrt{d}$, $a = m$, one obtains

$$\sum_{d \mid m} \frac{1}{\sqrt{d}} = \prod_{p \mid m} \left[1 + \frac{1}{\sqrt{p}} + \frac{1}{(\sqrt{p})^2} + \cdots + \frac{1}{(\sqrt{p})^\alpha}\right], \tag{2.69}$$

and hence

$$\sum_{d \mid m} \frac{1}{\sqrt{d}} < \prod_{p \mid m} \left[1 + \frac{1}{\sqrt{p}} + \frac{1}{(\sqrt{p})^2} + \cdots\right] = \prod_{p \mid m} \frac{\sqrt{p}}{\sqrt{p}-1}. \tag{2.70}$$

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

$$\sum_{d \mid m} \frac{1}{\sqrt{d}} \leqq (2 + \sqrt{2})^{\nu(m)} \tag{2.71}$$

Equations 2.66 and 2.71 now yield

$$S < \frac{\sqrt{m}}{\sqrt{2}\pi^2} (10 \ln^2 t + 7.4 \ln t \cdot \ln m)(2 + \sqrt{2})^{\nu(m)}. \tag{2.72}$$

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

LEMMA 9. *For $t \geqq 3$, one has*

$$\frac{\sqrt{m}}{\sqrt{2}\pi^2} \sum_{1 \leqq h \leqq t} \sum_{\substack{1 \leqq l \leqq t \\ h \neq l}} \frac{1}{hl} \sqrt{(h - l, m)}$$

$$< \frac{\sqrt{m}}{\pi^2} (8.52 \ln^2 t + 2.84 \ln t \cdot \ln m)(2 + \sqrt{2})^{\nu(m)}.$$

Proof. In abbreviation, define S by

$$S = \frac{\sqrt{m}}{\sqrt{2}\pi^2} \sum_{1 \leqq h \leqq t} \sum_{\substack{1 \leqq l \leqq t \\ h \neq l}} \frac{1}{hl} \sqrt{(h - l, m)}. \tag{2.73}$$

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

$$S = \frac{\sqrt{m}}{\sqrt{2}\pi^2} \sum_{d \mid m} \sqrt{d} \sum_{\substack{1 \leqq h \leqq t \\ (h-l,m)=d \\ h \neq l}} \sum_{1 \leqq l \leqq t} \frac{1}{hl} \tag{2.74}$$

Define $S'(d)$ by

$$S'(d) = \sum_{\substack{1 \leqq h \leqq t \\ d \mid h-l \\ h \neq l}} \sum_{1 \leqq l \leqq t} \frac{1}{hl}, \tag{2.75}$$

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

$$S \leqq \frac{\sqrt{m}}{\sqrt{2}\pi^2} \sum_{d \mid m} \sqrt{d}\, S'(d). \tag{2.76}$$

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.

$$S_r = \sum_{\substack{1 \leqq h \leqq t \\ h \equiv r \pmod d \\ l \equiv r \pmod d \\ h \neq l}} \sum_{1 \leqq l \leqq t} \frac{1}{hl}, \tag{2.77}$$

then

$$S'(d) = \sum_{r=0}^{d-1} S_r. \tag{2.78}$$

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

$$S_0 \leqq \frac{1}{d^2}\left(\sum_{1 \leqq c \leqq t/d} \frac{1}{c}\right)^2 < \frac{4 \ln^2 t}{d^2}. \tag{2.79}$$

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

$$S_r = \sum_{\substack{0 \leqq c \leqq \frac{t-r}{d} \\ c \neq e}} \sum_{0 \leqq e \leqq \frac{t-r}{d}} \frac{1}{(cd + r)(ed + r)}. \tag{2.80}$$

Due to the symmetry of the sum in Equation 2.80

$$S_r \leqq 2 \sum_{0 \leqq c \leqq \frac{t-r}{d}} \frac{1}{cd + r} \cdot \sum_{1 \leqq e \leqq \frac{t-r}{d}} \frac{1}{ed + r}. \tag{2.81}$$

Equation 2.57 yields

$$\sum_{0 \leqq c \leqq \frac{t-r}{d}} \frac{1}{cd + r} < \frac{1}{r} + \frac{\ln t}{d}; \tag{2.82}$$

further

$$\sum_{1 \leqq e \leqq \frac{t-r}{d}} \frac{1}{ed + r} < \frac{1}{d} \sum_{1 \leqq e \leqq t} \frac{1}{e} < \frac{1}{d}(1 + \ln t) < \frac{2 \ln t}{d}, \tag{2.83}$$

and hence,

$$S_r < \frac{4 \ln t}{rd} + \frac{4 \ln^2 t}{d^2}. \tag{2.84}$$

Since $1 \leqq d \leqq m$ and

$$\sum_{r=1}^{d-1} \frac{1}{r} < 1 + \ln m, \tag{2.85}$$

Equations 2.78 and 2.84 yield

$$S'(d) < \frac{12 \ln^2 t}{d} + \frac{4 \ln t \cdot \ln m}{d}. \tag{2.86}$$

From Equations 2.76 and 2.86, one now has

$$S < \frac{\sqrt{m}}{\sqrt{2}\pi^2}(12 \ln^2 t + 4 \ln t \cdot \ln m) \sum_{d \mid m} \frac{1}{\sqrt{d}}. \tag{2.87}$$

Equation 2.71 and the inequality $1/\sqrt{2} < .71$ yield the result of the lemma.

Let $A_r(m)$ designate the number of solutions of the congruence

$$aj^2 \equiv r (\mathrm{mod}\ m) \tag{2.88}$$

then Lemma 10 provides an estimate for $A_r(m)$ which is needed in the estimation of the sums S_f, S_g.

LEMMA 10. $(a, m) = 1$

$$\Rightarrow A_r(m) \leqq 2^{\nu(m)+1}\sqrt{(r, m)}.$$

Proof. Let A designate the number of solutions of the congruence

$$j^2 \equiv \sigma(\text{mod } m), \tag{2.89}$$

and let

$$m = 2^{\alpha}P_1^{\alpha_1}\cdots P_k^{\alpha_k} \tag{2.90}$$

be the canonical factorization of m with

$$\alpha \geqq 0, \qquad \alpha_l > 0, \qquad 1 \leqq l \leqq k \tag{2.91}$$

and the P_l odd primes. Then by the Chinese remainder theorem,

$$A = T\prod_{l=1}^{k} T_l \tag{2.92}$$

in which T_l is the number of solutions of $j^2 \equiv \sigma(\text{mod } p_l^{\alpha_l})$, and T is the number of solutions of $j^2 \equiv \sigma(\text{mod } 2^{\alpha})$. Consider the congruence

$$j^2 \equiv \sigma(\text{mod } p^{\beta}). \tag{2.93}$$

If $p^{\beta} \mid \sigma$ then the congruence has one solution i.e. $j \equiv 0(\text{mod } p^{\beta})$. Accordingly, let

$$(\sigma, p^{\beta}) = p^{2\gamma+\delta}, \qquad 0 \leqq \delta \leqq 1, \tag{2.94}$$

in which it is now supposed that $2\gamma + \delta < \beta$. Divide Equation 2.93 by $p^{2\gamma}$, then

$$j'^2 \equiv \sigma'(\text{mod } p^{\beta-2\gamma}) \tag{2.95}$$

in which

$$j = p^{\gamma}j', \qquad \sigma = p^{2\gamma}\sigma'. \tag{2.96}$$

One must have $\delta = 0$; otherwise, let $\delta = 1$ then $\sigma' = pq$, $p \nmid q$, $\beta - 2\gamma \geqq 2$, and

$$j'^2 \equiv pq(\text{mod } p^{\beta-2\gamma}). \tag{2.97}$$

Sin $p \mid pq$, $p \mid p^{\beta-2\gamma}$, one has $p \mid j'^2$; hence $p^2 \mid j'^2$. Also, since $p^2 \mid p^{\beta-2\gamma}$ it follows that $p^2 \mid pq$ which is impossible. Thus $\delta = 0$ and $(\sigma', p) = 1$. Let j_0' be a solution of Equation 2.95 then

$$(j_0' + p^{\beta-2\gamma}t)^2 \equiv \sigma'(\text{mod } p^{\beta-2\gamma}) \tag{2.98}$$

where t is an arbitrary integer. Multiplying Equation 2.98 by $p^{2\gamma}$, one obtains

$$(j_0 + p^{\beta-\gamma}t)^2 \equiv \sigma(\text{mod } p^{\beta}) \tag{2.99}$$

in which

$$j_0 = p^{\gamma}j_0', \tag{2.100}$$

and

$$j_0^2 \equiv \sigma(\text{mod } p^{\beta}). \tag{2.101}$$

Since for all t satisfying $0 \leqq t < p^\gamma$, one obtains solutions of Equation 2.93, there are p^γ solutions of Equation 2.93 for each solution of Equation 2.95. Since $(\sigma', p) = 1$, the number of solutions of Equation 2.95 does not exceed 2 when p is odd, and does not exceed 4 when $p = 2$ [3]. Thus

$$\begin{aligned} T_l &\leqq 2p^\gamma, \qquad \beta = \alpha_l, \\ T &\leqq 4\cdot 2^\gamma, \qquad \beta = \alpha. \end{aligned} \tag{2.102}$$

From Equation 2.94, one has

$$p^\gamma \leqq \sqrt{(\sigma, p^\beta)}; \tag{2.103}$$

thus, Equation 2.102 may be written

$$\begin{aligned} T_l &\leqq 2\sqrt{(\sigma, p_l{}^{\alpha_l})}, \\ T &\leqq 4\sqrt{(\sigma, 2^\alpha)}. \end{aligned} \tag{2.104}$$

Let m be odd, then

$$A = \prod_{l=1}^{k} T_l < 2^k \sqrt{\prod_{l=1}^{k} (\sigma, p_l{}^{\alpha_l})} = 2^{\nu(m)}\sqrt{(\sigma, m)}. \tag{2.105}$$

If m is even, then

$$A = T \prod_{l=1}^{k} T_l < 2^{k+2} \sqrt{(\sigma, 2^\alpha) \prod_{l=1}^{k} (\sigma, p_1{}^{\alpha_l})} = 2^{\nu(m)+1}\sqrt{(\sigma, m)}. \tag{2.106}$$

Thus in all cases

$$A \leqq 2^{\nu(m)+1}\sqrt{(\sigma, m)}. \tag{2.107}$$

Since $(a, m) = 1$, one has

$$(\sigma, m) = (r, m) \tag{2.108}$$

and hence the estimate of the lemma.

LEMMA 11. $(a, m) = 1$, $0 \leqq \alpha < 1$, $0 \leqq \beta < 1$, $m \geqq 2\pi t$

$$\Rightarrow S_f < 8(4 + 2\sqrt{2})^{\nu(m)} \left[\sqrt{m} + \frac{m \ln m}{\pi t}\right],$$

$$S_g < 8(4 + 2\sqrt{2})^{\nu(m)} \left[\sqrt{m} + \frac{m \ln m}{\pi t}\right].$$

Proof. Consider, in the sum

$$S_f = \sum_{j=0}^{m-1} \min\left(1, \frac{1}{2\pi t \left\| \frac{a}{m} j^2 - \alpha \right\|}\right), \tag{2.109}$$

regrouping the terms so that all j for which

$$aj^2 \equiv r \pmod m, \qquad 0 \leqq r < m \tag{2.110}$$

constitute a group indexed by r, then

$$S_f = \sum_{r=0}^{m-1} A_r(m) \min\left(1, \frac{1}{2\pi t \left\| \frac{r}{m} - \alpha \right\|}\right). \tag{2.111}$$

The estimate of Lemma 10 yields

$$S_f \leqq 2^{\nu(m)+1} \sum_{r=0}^{m-1} \sqrt{(r, m)} \min\left(1, \frac{1}{2\pi t \left\| \frac{r}{m} - \alpha \right\|}\right). \tag{2.112}$$

Let r be restricted so that $(r, m) = d$, then

$$S_f \leqq 2^{\nu(m)+1} \sum_{d \mid m} \sqrt{d} \sum_{\substack{0 \leqq r < m \\ (r,m)=d}} \min\left(1, \frac{1}{2\pi t \left\| \frac{r}{m} - \alpha \right\|}\right). \tag{2.113}$$

The set of integers r satisfying $(r, m) = d$ is included in the set $d \mid r$, hence

$$S_f \leqq 2^{\nu(m)+1} \sum_{d \mid m} \sqrt{d} \sum_{\substack{0 \leqq r < m \\ d \mid r}} \min\left(1, \frac{1}{2\pi t \left\| \frac{r}{m} - \alpha \right\|}\right). \tag{2.114}$$

Introducing the summation variable c by $r = dc$ and setting $d' = m/d$, one has

$$S_f \leqq 2^{\nu(m)+1} \sum_{d \mid m} \sqrt{d} \sum_{0 \leqq c < d'} \min\left(1, \frac{1}{2\pi t \left\| \frac{c}{d'} - \alpha \right\|}\right). \tag{2.115}$$

Let

$$S = \sum_{0 \leqq c < d'} \min\left(1, \frac{1}{2\pi t \left\| \frac{c}{d'} - \alpha \right\|}\right). \tag{2.116}$$

Then the sum S will be estimated by consideration of four cases.

Case 1. $-1 < \frac{c}{d'} - \alpha \leqq -\frac{1}{2}$.

One has

$$\left\| \frac{c}{d'} - \alpha \right\| = 1 + \frac{c}{d'} - \alpha, \tag{2.117}$$

$$\begin{aligned} \sum_{0 \leqq c \leqq d'(\alpha - \frac{1}{2})} \min\left(1, \frac{1}{2\pi t\left(1 + \frac{c}{d'} - \alpha\right)}\right) &\leqq 1 + \int_0^{d'(\alpha-\frac{1}{2})} \min\left(1, \frac{1}{2\pi t\left(1 + \frac{x}{d'} - \alpha\right)}\right) dx, \\ &< 1 + d' \int_0^{\frac{1}{2}} \min\left(1, \frac{1}{2\pi t u}\right) du, \\ &< 1 + \frac{d' \ln \pi t}{\pi t}. \end{aligned} \tag{2.118}$$

Case 2. $-\frac{1}{2} < \frac{c}{d'} - \alpha \leqq 0$.

One has

$$\left\| \frac{c}{d'} - \alpha \right\| = \alpha - \frac{c}{d'}, \tag{2.119}$$

and

$$\begin{aligned} \sum_{0 \leqq c \leqq d'\alpha} \min\left(1, \frac{1}{2\pi t\left(\alpha - \frac{c}{d'}\right)}\right) &\leqq 1 + \int_0^{d'\alpha} \min\left(1, \frac{1}{2\pi t\left(\alpha - \frac{x}{d'}\right)}\right) dx, \\ &< 1 + d' \int_0^1 \min\left(1, \frac{1}{2\pi t u}\right) du, \\ &< 1 + \frac{d' \ln 2\pi t}{\pi t}. \end{aligned} \tag{2.120}$$

Case 3. $0 < \dfrac{c}{d'} - \alpha \leqq \dfrac{1}{2}$

One has

$$\left\| \frac{c}{d'} - \alpha \right\| = \frac{c}{d'} - \alpha, \tag{2.121}$$

and

$$\begin{aligned} \sum_{d'\alpha < c < d'} \min\left(1, \frac{1}{2\pi t\left(\frac{c}{d'} - \alpha\right)}\right) &\leqq 1 + \int_{d'\alpha}^{d'} \min\left(1, \frac{1}{2\pi t\left(\frac{x}{d'} - \alpha\right)}\right) dx, \\ &\leqq 1 + d' \int_0^1 \min\left(1, \frac{1}{2\pi t u}\right) du, \\ &< 1 + \frac{d' \ln 2\pi t}{\pi t}. \end{aligned} \tag{2.122}$$

Case 4. $\dfrac{1}{2} < \dfrac{c}{d'} - \alpha < 1.$

One has

$$\left\| \frac{c}{d'} - \alpha \right\| = 1 - \frac{c}{d'} + \alpha, \tag{2.123}$$

$$\begin{aligned} &\sum_{d'(\alpha + \frac{1}{2}) < c < d'} \min\left(1, \frac{1}{2\pi t\left(1 - \frac{c}{d'} + \alpha\right)}\right) \\ &\qquad \leqq 1 + \int_{d'(\alpha+\frac{1}{2})}^{d'} \min\left(1, \frac{1}{2\pi t\left(1 - \frac{x}{d'} + \alpha\right)}\right) dx, \\ &\qquad \leqq 1 + d' \int_0^{\frac{1}{2}} \min\left(1, \frac{1}{2\pi t u}\right) du, \\ &\qquad < 1 + \frac{d' \ln \pi t}{\pi t}. \end{aligned} \tag{2.124}$$

Thus combining the estimates obtained in the above four cases, one has

$$S < 4 + 4\frac{d' \ln 2\pi t}{\pi t} \tag{2.125}$$

and hence

$$S_f < 8.2^{\nu(m)} \sum_{d|m} \sqrt{d}\left[1 + \frac{m \ln m}{\pi t d}\right] \tag{2.126}$$

where use was made of the inequality $m \geqq 2\pi t$. Equation 2.68 permits the following transformation of the sum $\sum_{d|m} \sqrt{d}$

$$\sum_{d|m} \sqrt{d} = \prod_{p|m} [1 + \sqrt{p} + \sqrt{p^2} + \cdots + \sqrt{p^\alpha}] \tag{2.127}$$

in which the product is over the prime divisors p of m. Since

$$\begin{aligned} 1 + \sqrt{p} + \sqrt{p^2} + \cdots + \sqrt{p^\alpha} &= \frac{\sqrt{p^{\alpha+1}} - 1}{\sqrt{p} - 1} \\ &< \sqrt{p^\alpha}\frac{\sqrt{p}}{\sqrt{p} - 1} \leqq (2 + \sqrt{2})\sqrt{p^\alpha}, \end{aligned} \tag{2.128}$$

one obtains

$$\sum_{d|m} \sqrt{d} < (2 + \sqrt{2})^{\nu(m)} \sqrt{m}. \tag{2.129}$$

Thus

$$S_f < 8(4 + 2\sqrt{2})^{\nu(m)} \sqrt{m} + \frac{8.2^{\nu(m)}\, m \ln m}{\pi t} \sum_{d|m} \frac{1}{\sqrt{d}}. \tag{2.130}$$

Use of Equation 2.71 yields

$$S_f < 8(4 + 2\sqrt{2})^{\nu(m)} \left[\sqrt{m} + \frac{m \ln m}{\pi t}\right]. \tag{2.131}$$

For the sum S_g, one has

$$S_g = \sum_{j=0}^{m-1} \min\left(1, \frac{1}{2\pi t \left\| \frac{a}{m}(j + \tau)^2 - \beta \right\|}\right) = \sum_{j=0}^{m-1} \min\left(1, \frac{1}{2\pi t \left\| \frac{a}{m} j^2 - \beta \right\|}\right) \tag{2.132}$$

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. $(a, m) = 1$, $m \geqq 36$, $1 \leqq \tau < \sqrt{m}$, $0 \leqq \alpha < 1$, $0 \leqq \beta < 1$,

$$\Rightarrow \left| \sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2 - \alpha\right) \rho\left(\frac{a}{m}(j + \tau)^2 - \beta\right) \right| < \sqrt{m}[.81(2 + \sqrt{2})^{\nu(m)} \ln^2 m + 33(4 + 2\sqrt{2})^{\nu(m)} \ln m].$$

Proof. Lemmas 7, 8, 9, and 11 yield

$$\begin{aligned} |R| < \frac{\sqrt{m}}{\pi^2} &[15 \cdot 62 \ln^2 t + 8.10 \ln t \cdot \ln m](2 + \sqrt{2})^{\nu(m)} \\ &+ 40(4 + 2\sqrt{2})^{\nu(m)} \left[\sqrt{m} + \frac{m \ln m}{\pi t}\right]. \end{aligned} \tag{2.133}$$

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

$$|R| < \sqrt{m}[1.59 \ln^2 t + .823 \ln t \cdot \ln m](2 + \sqrt{2})^{\nu(m)} + 40(4 + 2\sqrt{2})^{\nu(m)}\left[\sqrt{m} + \frac{m \ln m}{\pi t}\right]. \tag{2.134}$$

Choose

$$t = \tfrac{1}{2}\sqrt{m}, \tag{2.135}$$

then, since $\ln t < \frac{1}{2} \ln m$ and $\pi > 3.14$,

$$|R| < \sqrt{m}[.81(2 + \sqrt{2})^{\nu(m)} \ln^2 m + 40(4 + 2\sqrt{2})^{\nu(m)} + 26(4 + 2\sqrt{2})^{\nu(m)} \ln m]. \tag{2.136}$$

One has

$$40(4 + 2\sqrt{2})^{\nu(m)} + 26(4 + 2\sqrt{2})^{\nu(m)} \ln m = (4 + 2\sqrt{2})^{\nu(m)} \ln m \cdot \left(\frac{40}{\ln m} + 26\right). \tag{2.137}$$

Since $m \geqq 36$, $\ln m \geqq \ln 36 > 5.88$, one has

$$(40 + 26 \ln m)(4 + 2\sqrt{2})^{\nu(m)} < 33(4 + 2\sqrt{2})^{\nu(m)} \ln m, \tag{2.138}$$

and hence

$$|R| < \sqrt{m}[.81(2 + \sqrt{2})^{\nu(m)} \ln^2 m + 33(4 + 2\sqrt{2})^{\nu(m)} \ln m]. \tag{2.139}$$

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

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

THEOREM 2. $(a, m) = 1$, $m \geqq 36$, $1 \leqq \tau < \sqrt{m}$

$$\Rightarrow |\psi(\tau)| < m^{-\frac{1}{2}}[.81(2 + \sqrt{2})^{\nu(m)} \ln^2 m + 33(4 + 2\sqrt{2})^{\nu(m)} \ln m].$$

Consider the simultaneous Diophantine inequalities

$$0 \leqq \left\{\frac{a}{m} j^2\right\} < \alpha, \qquad 0 \leqq \left\{\frac{a}{m}(j + \tau)^2\right\} < \beta, \qquad 0 \leqq j < m. \tag{2.140}$$

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

$$G(\alpha, \beta) = \frac{T(\alpha, \beta)}{m} \tag{2.141}$$

is the joint distribution function of the sequences $\left\{\frac{a}{m} j^2\right\}, \left\{\frac{a}{m}(j + \tau)^2\right\}$. If the sequences $\left\{\frac{a}{m} j^2\right\}, \left\{\frac{a}{m}(j + \tau)^2\right\}$ were independently equidistributed over (0, 1), one would have $G(\alpha, \beta) = \alpha\beta$. It is the present object to determine the devia-

tion of $G(\alpha, \beta)$ from the desired joint distribution $\alpha\beta$. For this purpose, let

$$H_\alpha(x) = \alpha + \rho(x) - \rho(x - \alpha), \tag{2.142}$$

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

$$\begin{aligned} H_\alpha(x) &= 1, & 0 \leqq x < \alpha, \\ &= 0, & \alpha \leqq x < 1. \end{aligned} \tag{2.143}$$

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

$$T(\alpha, \beta) = \sum_{j=0}^{m-1} H_\alpha\left(\frac{a}{m} j^2\right) H_\beta\left(\frac{a}{m}(j + \tau)^2\right). \tag{2.144}$$

LEMMA 12.

$$\begin{aligned} T(\alpha, \beta) = {} & \alpha\beta m + \beta \sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2\right) - \beta \sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2 - \alpha\right) \\ & + \alpha \sum_{j=0}^{m-1} \rho\left(\frac{a}{m}(j + \tau)^2\right) - \alpha \sum_{j=0}^{m-1} \rho\left(\frac{a}{m}(j + \tau)^2 - \beta\right) \\ & + \sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2\right) \rho\left(\frac{a}{m}(j + \tau)^2\right) - \sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2 - \alpha\right) \rho\left(\frac{a}{m}(j + \tau)^2\right) \\ & - \sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2\right) \rho\left(\frac{a}{m}(j + \tau)^2 - \beta\right) + \sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2 - \alpha\right) \rho\left(\frac{a}{m}(j + \tau)^2 - \beta\right). \end{aligned}$$

Proof. Use of Equations 2.142 and 2.144.

LEMMA 13. $(a, m) = 1$, $m \geqq 36$, $1 \leqq \tau < \sqrt{m}$, $0 \leqq \alpha < 1$, $0 \leqq \beta < 1$,

$$\begin{aligned} \Rightarrow |\, T(\alpha, \beta) - \alpha\beta m \,| < {} & 2\left|\sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2\right)\right| \\ & + \left|\sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2 - \alpha\right)\right| + \left|\sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2 - \beta\right)\right| \\ & + \sqrt{m}[3.24(2 + \sqrt{2})^{\nu(m)} \ln^2 m + 132(4 + 2\sqrt{2})^{\nu(m)} \ln m]. \end{aligned}$$

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

$$\sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2\right) = \sum_{j=0}^{m-1} \left(\frac{a}{m}(j + \tau)^2\right), \tag{2.145}$$

and

$$\sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2 - \beta\right) = \sum_{j=0}^{m-1} \left(\frac{a}{m}(j + \tau)^2 - \beta\right), \tag{2.146}$$

the lemma follows.

In order to estimate the sum of the ρ-functions in Lemma 13, the following lemmas are required.

LEMMA 14. $(a, m) = 1$, $0 \leqq \alpha < 1$,

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

Proof. Let

$$(h, m) = d$$
$$h' = \frac{h}{d}, \tag{2.147}$$
$$m' = \frac{m}{d},$$

and

$$S = \sum_{j=0}^{m-1} e\left(\frac{ha}{m} j^2 - h\alpha\right), \tag{2.148}$$

then

$$|S| = \left|\sum_{j=0}^{m-1} e\left(\frac{ha}{m} j^2\right)\right| = d\left|\sum_{j=0}^{m'-1} e\left(\frac{h'a}{m'} j^2\right)\right|. \tag{2.149}$$

One has

$$\begin{aligned} |S|^2 &= d^2 \sum_{k=0}^{m'-1} \sum_{j=0}^{m'-1} e\left(\frac{h'a}{m'} j^2 - \frac{h'a}{m'} k^2\right) \\ &= d^2 \sum_{k=0}^{m'-1} \sum_{j=k}^{m'-1+k} e\left(\frac{h'a}{m'} j^2 - \frac{h'a}{m'} k^2\right). \end{aligned} \tag{2.150}$$

Introduce a new summation variable ν by

$$j = k + \nu, \tag{2.151}$$

then

$$|S|^2 = d^2 \sum_{\nu=0}^{m'-1} \sum_{k=0}^{m'-1} e\left(\frac{2h'a}{m'} \nu k\right) e\left(\frac{h'a}{m'} \nu^2\right) \leqq d^2 \sum_{\nu=0}^{m'-1} \left|\sum_{k=0}^{m'-1} e\left(\frac{2h'a}{m'} \nu k\right)\right|. \tag{2.152}$$

By direct summation, one obtains

$$\begin{aligned} \sum_{k=0}^{m'-1} e\left(\frac{2h'a}{m'} \nu k\right) &= 0, && m' \nmid 2h'a\nu, \\ &= m', && m' \mid 2h'a\nu. \end{aligned} \tag{2.153}$$

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,

$$|S|^2 \leqq 2d^2 m' = 2md. \tag{2.154}$$

The lemma follows on taking the square root.

LEMMA 15. $(a, m) = 1$, $m \geqq 36$, $0 \leqq \alpha < 1$,

$$\Rightarrow \left|\sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2 - \alpha\right)\right| < \frac{\sqrt{2m}}{\pi} \sum_{1 \leqq h \leqq t} \frac{1}{h} \sqrt{(h, m)} + 64.7\sqrt{m}(4 + 2\sqrt{2})^{\nu(m)} \ln m.$$

Proof. Use of Lemma 1 yields

$$\left|\sum_{j=0}^{m-1}\rho\left(\frac{a}{m}j^2-\alpha\right)\right| < \sum_{1\leqq h\leqq t}\frac{1}{\pi h}\left|\sum_{j=0}^{m-1}e\left(\frac{ha}{m}j^2\right)\right| + \sum_{j=0}^{m-1}\min\left(1,\frac{1}{2\pi t\left\|\frac{a}{m}j^2-\alpha\right\|}\right). \tag{2.155}$$

Setting $t = \frac{1}{2}\sqrt{m}$ and using Lemma 11, one obtains

$$\left|\sum_{j=0}^{m-1}\rho\left(\frac{a}{m}j^2-\alpha\right)\right| < \sum_{1\leqq h\leqq \frac{1}{2}\sqrt{m}}\frac{1}{\pi h}\left|\sum_{j=0}^{m-1}e\left(\frac{ha}{m}j^2\right)\right| + 8(4+2\sqrt{2})^{\nu(m)}\sqrt{m}\left[1+\frac{2}{\pi}\ln m\right]. \tag{2.156}$$

Since $m \geqq 36$, one has $\ln m > 5.88$, hence

$$\left|\sum_{j=0}^{m-1}\left(\frac{a}{m}j^2-\alpha\right)\right| < \sum_{1\leqq h\leqq \frac{1}{2}\sqrt{m}}\frac{1}{\pi h}\left|\sum_{j=0}^{m-1}e\left(\frac{ha}{m}j^2\right)\right| + 64.7\sqrt{m}(4+2\sqrt{2})^{\nu(m)}\ln m \tag{2.157}$$

The lemma now follows on employing Lemma 14.

LEMMA 16. $(a, m) = 1$, $m \geqq 36$, $0 \leqq \alpha < 1$,

$$\Rightarrow \left|\sum_{j=0}^{m-1}\rho\left(\frac{a}{m}j^2-\alpha\right)\right| < 64.9\sqrt{m}(4+2\sqrt{2})^{\nu(m)}\ln m.$$

Proof. One has

$$\frac{\sqrt{2m}}{\pi}\sum_{1\leqq h\leqq\frac{1}{2}\sqrt{m}}\frac{1}{h}\sqrt{(h,m)} = \frac{\sqrt{2m}}{\pi}\sum_{d\mid m}\sqrt{d}\sum_{\substack{1\leqq h\leqq\frac{1}{2}\sqrt{m}\\(h,m)=d}}\frac{1}{h} \leqq \frac{\sqrt{2m}}{\pi}\sum_{d\mid m}\sqrt{d}\sum_{\substack{1\leqq h\leqq\frac{1}{2}\sqrt{m}\\d\mid h}}\frac{1}{h}. \tag{2.158}$$

Let $h = cd$, then,

$$\frac{\sqrt{2m}}{\pi}\sum_{d\mid m}\sqrt{d}\sum_{\substack{1\leqq h\leqq\frac{1}{2}\sqrt{m}\\d\mid h}}\frac{1}{h} \leqq \frac{\sqrt{2m}}{\pi}\sum_{d\mid m}\frac{1}{\sqrt{d}}\sum_{1\leqq c\leqq\frac{1}{2}\sqrt{m}}\frac{1}{c} < \sqrt{m}(.15+.27\ln m)\sum_{d\mid m}\frac{1}{\sqrt{d}}. \tag{2.159}$$

Use of Equation 2.71 now yields

$$\frac{\sqrt{2m}}{\pi}\sum_{1\leqq h\leqq\frac{1}{2}\sqrt{m}}\frac{1}{h}\sqrt{(h,m)} < \sqrt{m}(.15+.27\ln m)(2+\sqrt{2})^{\nu(m)}. \tag{2.160}$$

Since $m \geqq 36$, one has

$$.15 + .27\ln m < .296\ln m, \tag{2.161}$$

and hence

$$\frac{\sqrt{2m}}{\pi} \sum_{1 \leqq h \leqq \frac{1}{2}\sqrt{m}} \frac{1}{h} \sqrt{(h, m)} < .296\sqrt{m}(2 + \sqrt{2})^{\nu(m)} \ln m, \tag{2.162}$$

Lemma 15 now yields

$$\left| \sum_{j=0}^{m-1} \rho\left(\frac{a}{m} j^2 - \alpha\right) \right| < .296\sqrt{m}(2 + 2\sqrt{2})^{\nu(m)} \ln m + 64.7\sqrt{m}(4 + 2\sqrt{2})^{\nu(m)} \ln m. \tag{2.163}$$

Since

$$.296(2 + \sqrt{2})^{\nu(m)} + 64.7(4 + 2\sqrt{2})^{\nu(m)} < 64.9(4 + 2\sqrt{2})^{\nu(m)} \tag{2.164}$$

The lemma follows.

THEOREM 3. $(a, m) = 1, m \geqq 36, 1 \leqq \tau < \sqrt{m},$

$\Rightarrow | G(\alpha, \beta) - \alpha\beta | < m^{-\frac{1}{2}}[3.24(2 + \sqrt{2})^{\nu(m)} \ln^2 m + 392(4 + 2\sqrt{2})^{\nu(m)} \ln m].$

Proof. Use of Lemmas 13 and 16.

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

System Development Corporation
Santa Monica, California, and
Fairleigh Dickinson University
Rutherford, New Jersey

1. G. H. HARDY, *Divergent Series*, Oxford University Press, Amen House, Great Britain, 1949.
2. JOEL N. FRANKLIN, "Deterministic simulation of random processes," *Math. Comp.*, v. 17, 1963, p. 28–59.
3. I. M. VINOGRADOV, *Elements of Number Theory*, Dover Publications, Inc., New York, 1954.