Some Theorems Concerning Pseudo-Random Numbers

By D. L. Jagerman

Some quantitative theorems concerning the use of pseudo-random numbers will be presented. Let $x_1, \cdots, x_P$ be a given sequence satisfying

$$(1) \qquad 0 \leq x_j \leq 1, \qquad 1 \leq j \leq P,$$

and $f(x)$ a real, integrable function; then the first four theorems estimate the quantity

$$(2) \qquad \left| \frac{1}{P} \sum_{j=1}^{P} f(x_j) - \int_0^1 f(x)\, dx \right| .$$

Further restrictions on the sequence x_j will be imposed through a trigonometric sum. Let $n \neq 0$ be an integer, and let

$$(3) \qquad e(x) = e^{i2\pi x};$$

then effective estimates for the size of

$$(4) \qquad \left| \sum_{j=1}^{P} e(nx_j) \right|$$

will be required. Restrictions on the function $f(x)$ will be imposed by means of its Fourier coefficients. Thus, let $f(x)$ be given by

$$(5) \qquad f(x) = \int_0^1 f(u)\, du + \sum_{n=-\infty}^{\infty}{}' c_n\, e(nx),$$

in which the prime shows the absence of the term $n = 0$; then growth restrictions on c_n will be required. The fifth theorem is concerned with multiply sequences; it provides an estimate for the deviation of such a sequence from the ideal uniformly distributed case. The symbols $[x]$ and $\{x\}$ will be used to denote the integral part and the fractional part of x, respectively.

THEOREM 1. $C > 0, K > 0, \alpha > 0, \beta < 1, \nu > 1 + \alpha \ni$

$$| c_n | \leq C\, | n |^{-\nu}, \qquad \left| \sum_{j=1}^{P} e(nx_j) \right| < K\, | n |^{\alpha}\, P^{\beta}$$

$$\Rightarrow \left| \frac{1}{P} \sum_{j=1}^{P} f(x_j) - \int_0^1 f(x)\, dx \right| < \frac{2KC(\nu - \alpha)}{\nu - \alpha - 1}\, P^{\beta-1}.$$

Proof. The Fourier series for $f(x)$ is

$$(6) \qquad f(x) = \sum_{n=-\infty}^{\infty} c_n e(nx)$$

Received December 28, 1964.

in which

$$c_n = \int_0^1 e(-nx)f(x)\,dx. \tag{7}$$

Thus, since the sequence x_j obeys the inequality $0 \leqq x_j \leqq 1$, one has

$$\frac{1}{P}\sum_{j=1}^{P} f(x_j) - \int_0^1 f(x)\,dx = \sum_{n=-\infty}^{\infty}{}' c_n \frac{1}{P}\sum_{j=1}^{P} e(nx_j). \tag{8}$$

Since $|c_n|$ and $|(1/P)\sum_{j=1}^{P} e(nx_j)|$ are even functions of n, (8) may be put in the form

$$\left|\frac{1}{P}\sum_{j=1}^{P} f(x_j) - \int_0^1 f(x)\,dx\right| \leqq 2\sum_{n=1}^{\infty} |c_n| \left|\frac{1}{P}\sum_{j=1}^{P} e(nx_j)\right|. \tag{9}$$

The conditions of the theorem imply

$$\left|\frac{1}{P}\sum_{j=1}^{P} f(x_j) - \int_0^1 f(x)\,dx\right| \leqq 2KCP^{\beta-1}\sum_{n=1}^{\infty}\frac{1}{n^{\nu-\alpha}}. \tag{10}$$

Since

$$\sum_{n=1}^{\infty}\frac{1}{n^{\nu-\alpha}} < 1 + \int_1^{\infty}\frac{dx}{x^{\nu-\alpha}} = \frac{\nu-\alpha}{\nu-\alpha-1}, \tag{11}$$

the theorem follows.

THEOREM 2. $C > 0, K > 0, \alpha > 0, \beta < 1, \nu = 1 + \alpha \ni$

$$|c_n| \leqq C|n|^{-\nu}, \qquad \left|\sum_{j=1}^{P} e(nx_j)\right| \leqq K|n|^{\alpha} P^{\beta}, \qquad P \geqq 3^{\alpha/(1-\beta)}$$

$$\Rightarrow \left|\frac{1}{P}\sum_{j=1}^{P} f(x_j) - \int_0^1 f(x)\,dx\right| < \frac{2C}{\alpha}P^{\beta-1}\left[2K(1-\beta)\ln P + \left(\frac{3}{2}\right)^{\alpha}\right].$$

Proof. The proof is the same as for Theorem 1 up to (9). One has

$$\left|\frac{1}{P}\sum_{j=1}^{P} f(x_j) - \int_0^1 f(x)\,dx\right| \leqq 2KCP^{\beta-1}\sum_{1\leqq n\leqq P^{(1-\beta)/\alpha}}\frac{1}{n^{\nu-\alpha}} + 2C\sum_{n>P^{(1-\beta)/\alpha}}\frac{1}{n^{\nu}}, \tag{12}$$

in which the estimate

$$\left|\frac{1}{P}\sum_{j=1}^{P} e(nx_j)\right| \leqq 1 \tag{13}$$

was used in the second sum. Since

$$\sum_{n>P^{(1-\beta)/\alpha}}\frac{1}{n^{\nu}} < \int_{[P^{(1-\beta)/\alpha}]}^{\infty}\frac{dx}{x^{\nu}} = \frac{1}{(\nu-1)[P^{(1-\beta)/\alpha}]^{\nu-1}}, \tag{14}$$

and

$$[P^{(1-\beta)/\alpha}] > P^{(1-\beta)/\alpha} - 1 = P^{(1-\beta)/\alpha}(1 - P^{-(1-\beta)/\alpha}) \geqq \tfrac{2}{3}P^{(1-\beta)/\alpha}, \tag{15}$$

one has

$$\sum_{n>P^{(1-\beta)/\alpha}}\frac{1}{n^{\nu}} < \frac{1}{\nu-1}\left(\frac{3}{2}\right)^{\nu-1} P^{-(1-\beta)(\nu-1)/\alpha}, \tag{16}$$

and, hence,

$$(17) \qquad 2C \sum_{n > P^{(1-\beta)/\alpha}} \frac{1}{n^\nu} < \frac{2C}{\alpha}\left(\frac{3}{2}\right)^\alpha P^{\beta-1}.$$

Also, since

$$(18) \qquad \sum_{1 \leqq n \leqq P^{(1-\beta)/\alpha}} \frac{1}{n^{\nu-\alpha}} < 1 + \int_1^{P^{(1-\beta)/\alpha}} \frac{dx}{x} = 1 + \frac{1-\beta}{\alpha} \ln P < 2\frac{1-\beta}{\alpha} \ln P,$$

substituting (17) and (18) into (12) establishes the theorem.

THEOREM 3. $C > 0, K > 0, \alpha > 0, \beta < 1, 1 < \nu < 1 + \alpha \ni$

$$| c_n | \leqq C | n |^{-\nu}, \qquad \left| \sum_{j=1}^P e(nx_j) \right| \leqq K | n |^\alpha P^\beta, \qquad P \geqq 3^{\alpha/(1-\beta)}$$

$$\Rightarrow \left| \frac{1}{P} \sum_{j=1}^P f(x_j) - \int_0^1 f(x)\, dx \right| < 2CP^{-(1-\beta)(\nu-1)/\alpha} \left[\frac{K}{1-\nu+\alpha} + \frac{1}{\nu-1}\left(\frac{3}{2}\right)^{\nu-1} \right].$$

Proof. The proof of this theorem is the same as that of Theorem 2 up to (16). One has

$$(19) \qquad \sum_{1 \leqq n \leqq P^{(1-\beta)/\alpha}} \frac{1}{n^{\nu-\alpha}} < \int_0^{P^{(1-\beta)/\alpha}} \frac{dx}{x^{\nu-\alpha}} = \frac{1}{1-\nu+\alpha} P^{(1-\beta)(1-\nu+\alpha)/\alpha}$$

and, hence, substituting (16) and (19) into (12) establishes the theorem.

THEOREM 4. $C > 0, K > 0, \alpha > 0, \beta < 1, \nu > 1, \nu < \alpha \ni$

$$| c_n | \leqq C | n |^{-\nu}, \qquad \left| \sum_{j=1}^P e(nx_j) \right| \leqq K | n |^\alpha P^\beta, \qquad P \geqq 3^{\alpha/(1-\beta)}$$

$$\Rightarrow \left| \frac{1}{P} \sum_{j=1}^P f(x_j) - \int_0^1 f(x)\, dx \right|$$
$$< 2CP^{-(1-\beta)(\nu-1)/\alpha} \left[\frac{K}{1-\nu+\alpha}\left(\frac{4}{3}\right)^{1-\nu+\alpha} + \frac{1}{\nu-1}\left(\frac{3}{2}\right)^{\nu-1} \right].$$

Proof. The proof of this theorem is the same as that of Theorem 2 up to (16). One has

$$(20) \qquad \begin{aligned} \sum_{1 \leqq n \leqq P^{(1-\beta)/\alpha}} \frac{1}{n^{\nu-\alpha}} &< \int_1^{P^{(1-\beta)/\alpha}} \frac{dx}{x^{\nu-\alpha}} < \frac{(P^{(1-\beta)/\alpha} + 1)^{1-\nu+\alpha}}{1-\nu+\alpha} \\ &\leqq \frac{1}{1-\nu+\alpha}\left(\frac{4}{3}\right)^{1-\nu+\alpha} P^{(1-\beta)(1-\nu+\alpha)/\alpha}. \end{aligned}$$

Substituting (16) and (20) into (12) establishes the theorem.

A multiply sequence is defined by the recurrence relation

$$(21) \qquad x_{j+1} = \left\{ \lambda x_j + \frac{\mu}{m} \right\}, \qquad j \geqq 0,$$

in which $\lambda > 1$, $m > 0$, $\mu \geqq 0$ are integers, and x_0 is arbitrarily chosen. Franklin [1] showed that, for almost all x_0, a multiply sequence is equidistributed. Let mx_0 be an integer which is relatively prime to m, then mx_j is the sequence of integers customarily employed as pseudo-random numbers. Inductively, one easily establishes the following explicit representation:

$$x_j = \left\{\lambda^j x_0 + \frac{\mu}{m}\frac{\lambda^j - 1}{\lambda - 1}\right\}. \tag{22}$$

If mx_0 is an integer, then the sequence x_j is clearly periodic in the sense that $x_{j+m} = x_j$ for all j; however, it is generally desirable that the sequence contain as many members which are incongruent modulo m as possible. This is accomplished by choosing for λ a primitive root modulo m. A statistical function of interest is the distribution function, $\omega(\alpha)$. Let P denote the period of the sequence; then, if $T(\alpha)$ is the number of elements of the sequence which do not exceed α,

$$\omega(\alpha) = \frac{T(\alpha)}{P}. \tag{23}$$

Since $\omega(\alpha) = 0$ for $\alpha \leqq 0$ and $\omega(\alpha) = 1$ for $\alpha \geqq 1$, it is convenient to restrict α so that $0 < \alpha < 1$. The following discontinuous function will aid in the determination of $\omega(\alpha)$. Let

$$\begin{aligned} H_\alpha(x) &= 1, \qquad 0 \leqq x < \alpha, \\ H_\alpha(x) &= 0, \qquad \alpha \leqq x < 1, \end{aligned} \tag{24}$$

and define $H_\alpha(x)$ for all x by periodic extension; then

$$\omega(\alpha) = \frac{1}{P}\sum_{j=1}^{P} H_\alpha(x_j). \tag{25}$$

The special case $\mu = 0$ of (22) will be studied in which λ is a primitive root modulo m and $P = \phi(m)$, where $\phi(m)$ is the totient. Thus

$$x_j = \{\lambda^j x_0\}, \tag{26}$$

and mx_0 is one of the numbers of a reduced residue system modulo m. In order to investigate the distribution function of this sequence, several lemmas are needed. Let

$$\rho(x) = \tfrac{1}{2} - \{x\}; \tag{27}$$

then:

LEMMA 1.

$$|\,\omega(\alpha) - \alpha\,| \leqq \left|\frac{1}{P}\sum_{j=1}^{P}\rho(x_j)\right| + \left|\frac{1}{P}\sum_{j=1}^{P}\rho(x_j - \alpha)\right|, \qquad 0 < \alpha < 1.$$

Proof. One has

$$H_\alpha(x) = \alpha + \rho(x) - \rho(x - \alpha), \tag{28}$$

which may be established by consideration of the two cases $0 \leqq x < \alpha$ and $\alpha \leqq x < 1$. Thus, from (25),

$$\omega(\alpha) = \alpha + \frac{1}{P}\sum_{j=1}^{P}\rho(x_j) - \frac{1}{P}\sum_{j=1}^{P}\rho(x_j - \alpha). \tag{29}$$

The lemma follows from (29).

LEMMA 2.

$$t > 0 \Rightarrow -\frac{1}{2t} + t\int_{-1/t}^{0} \rho(x+u)\,du \leqq \rho(x) \leqq \frac{1}{2t} + t\int_{0}^{1/t} \rho(x+u)\,du.$$

Proof. From the monotonicity of $[x]$, one has

$$t\int_{-1/t}^{0} [x+u]\,du \leqq [x] \leqq t\int_{0}^{1/t} [x+u]\,du. \tag{30}$$

Since

$$[x] = x - \tfrac{1}{2} + \rho(x), \tag{31}$$

substitution of this into (30) yields the lemma.

LEMMA 3. $t > 0$

$$\Rightarrow -\frac{1}{2t} + \sum_{n=-\infty}^{\infty} d_n e(nx) \leqq \rho(x) \leqq \sum_{n=-\infty}^{\infty} c_n e(nx) + \frac{1}{2t},$$

$$|c_n| = |d_n| \leqq \min\left(\frac{1}{2\pi|n|}, \frac{t}{2\pi^2 n^2}\right).$$

Proof. Use of the Fourier series

$$\rho(x) = \sum_{n=-\infty}^{\infty}{}' \frac{e(nx)}{i2\pi n} \tag{32}$$

yields

$$t\int_0^{1/t} \rho(x+u)\,du = \sum_{n=-\infty}^{\infty}{}' c_n e(nx), \qquad c_n = t\,\frac{1 - e\left(\frac{n}{t}\right)}{4\pi^2 n^2}. \tag{33}$$

Thus

$$|c_n| = \frac{t}{4\pi^2 n^2}\left|e\left(\frac{n}{t}\right) - 1\right| \leqq \frac{t}{2\pi^2 n^2}. \tag{34}$$

From the identity

$$e\left(\frac{n}{t}\right) - 1 = 2ie\left(\frac{n}{2t}\right)\sin\frac{\pi n}{t}, \tag{35}$$

one has

$$\left|e\left(\frac{n}{t}\right) - 1\right| \leqq \frac{2\pi|n|}{t}. \tag{36}$$

Applying (36) to (33), one has

$$|c_n| \leqq \frac{1}{2\pi|n|}. \tag{37}$$

Similarly,

$$(38)\qquad t\int_{-1/t}^{0} \rho(x+u)\,du = \sum_{n=-\infty}^{\infty}{}' d_n e(nx), \qquad d_n = t\,\frac{e\left(-\frac{n}{t}\right)-1}{4\pi^2 n^2}.$$

Equations (33) and (38) show that

$$(39)\qquad \bar{d}_n = -c_n$$

and, hence, that

$$(40)\qquad |\,d_n\,| = |\,c_n\,|.$$

Inequalities (34) and (37) are also valid for d_n; hence, the lemma is established.

LEMMA 4.

$$t > 0, \quad y_j \text{ real} \Rightarrow \left|\frac{1}{P}\sum_{j=1}^{P}\rho(y_j)\right| \leqq \frac{1}{P}\sum_{n=1}^{\infty}\min\left(\frac{1}{\pi n}, \frac{t}{\pi^2 n^2}\right)\left|\sum_{j=1}^{P} e(ny_j)\right| + \frac{1}{2t}.$$

Proof. In the inequalities of Lemma 3, x is replaced by y_j and summation is performed over j. Thus

$$(41)\qquad -\frac{1}{2t} + \frac{1}{P}\sum_{n=-\infty}^{\infty}{}' d_n \sum_{j=1}^{P} e(ny_j) \leqq \frac{1}{P}\sum_{j=1}^{P}\rho(y_j) \leqq \frac{1}{P}\sum_{n=-\infty}^{\infty}{}' c_n \sum_{j=1}^{P} e(ny_j) + \frac{1}{2t}$$

and, hence

$$(42)\qquad \begin{aligned} -\frac{1}{2t} - \frac{1}{P}\sum_{n=\infty}^{\infty}{}' \,|\,d_n\,|\left|\sum_{j=1}^{P} e(ny_j)\right| &\leqq \left|\frac{1}{P}\sum_{j=1}^{\infty}{}' \rho(y_j)\right| \\ &\leqq \frac{1}{P}\sum_{n=-\infty}^{\infty}{}' \,|\,c_n\,|\left|\sum_{j=1}^{P} e(ny_j)\right| + \frac{1}{2t}. \end{aligned}$$

From Lemma 3, one has $|\,c_n\,| = |\,d_n\,|$; also, $|\,c_n\,|$ and $|\,\sum_{j=1}^{P} e(ny_j)\,|$ are even functions of n, hence,

$$(43)\qquad \left|\frac{1}{P}\sum_{j=1}^{P}\rho(y_j)\right| \leqq \frac{2}{P}\sum_{n=1}^{\infty}|\,c_n\,|\left|\sum_{j=1}^{P} e(ny_j)\right| + \frac{1}{2t}.$$

Use of the inequality

$$(44)\qquad |\,c_n\,| \leqq \min\left(\frac{1}{2\pi n}, \frac{t}{2\pi^2 n^2}\right), \qquad n > 0,$$

yields the lemma.

It will be convenient to introduce the function $\delta_{n,d}$ defined by

$$(45)\qquad \begin{aligned} \delta_{n,d} &= 1, \qquad d|n, \\ \delta_{n,d} &= 0, \qquad d\nmid n. \end{aligned}$$

LEMMA 5.

$$x_j \textit{ is defined by } (26), P = \phi(m) \Rightarrow \left|\sum_{j=1}^{P} e(nx_j)\right| \leqq \sum_{d\,|\,m} d\delta_{n,d}.$$

Proof. Since λ is a primitive root modulo m, λ^j runs through a reduced residue system. Let

$$\lambda^j m x_0 \equiv r \pmod{m}, \tag{46}$$

where r is the least nonnegative residue; then r runs through a reduced residue system modulo m, and

$$\sum_{j=1}^{P} e(n\lambda^j x_0) = \sum_r e\left(\frac{nr}{m}\right). \tag{47}$$

The sum $\sum_r e(nr/m)$ is a Ramanujan sum whose value can be expressed in terms of the Möbius function, $\mu(n)$ [2]. Let $c_m(n)$ denote the Ramanujan sum; then one has

$$c_m(n) = \sum_{d\mid(m,n)} d\mu\left(\frac{m}{d}\right). \tag{48}$$

Thus

$$|c_m(n)| \leqq \sum_{d\mid(m,n)} d = \sum_{d\mid m} d\delta_{n,d}.$$

It is now possible to establish

THEOREM 5. $x_{j+1} = \{\lambda x_j\}$, $0 < x_0 < 1$, $m \geqq 3$, $(mx_0, m) = 1$, λ *is a primitive root modulo* m, $\omega(\alpha)$ *is the distribution function*, $P = \phi(m)$

$$\Rightarrow |\omega(\alpha) - \alpha| < \frac{4}{\pi}\sqrt{\frac{3\ln m}{P}}.$$

Proof. Use of Lemmas 1 and 4 yields

$$\left|\frac{1}{P}\sum_{j=1}^{P} \rho(x_j - \alpha)\right| \leqq \frac{1}{P}\sum_{n=1}^{\infty} \min\left(\frac{1}{\pi n}, \frac{t}{\pi^2 n^2}\right)\left|\sum_{j=1}^{P} e(nx_j)\right| + \frac{1}{2t}, \tag{49}$$

and

$$|\omega(\alpha) - \alpha| \leqq \frac{2}{P}\sum_{n=1}^{\infty} \min\left(\frac{1}{\pi n}, \frac{t}{\pi^2 n^2}\right)\left|\sum_{j=1}^{P} e(nx_j)\right| + \frac{1}{t}. \tag{50}$$

Lemma 5 is now used to provide an estimate for the trigonometric sum appearing in (50). Define the summation variable γ by $n = \gamma d$, then

$$|\omega(\alpha) - \alpha| \leqq \frac{2}{P}\sum_{d\mid m}\sum_{\gamma=1}^{\infty} \min\left(\frac{1}{\pi\gamma}, \frac{t}{\pi^2\gamma^2 d}\right) + \frac{1}{t}. \tag{51}$$

When

$$t \geqq \pi d, \tag{52}$$

one has

$$\sum_{\gamma=1}^{\infty} \min\left(\frac{1}{\pi\gamma}, \frac{t}{\pi^2\gamma^2 d}\right) = \sum_{1\leqq\gamma\leqq t/\pi d} \frac{1}{\pi\gamma} + \sum_{\gamma > t/\pi d} \frac{t}{\pi^2\gamma^2 d}. \tag{53}$$

Since

$$\sum_{1\leqq\gamma\leqq t/\pi d} \frac{1}{\gamma} < 1 + \int_1^{[t/\pi d]} \frac{dx}{x} \leqq 1 + \int_1^{t/\pi d} \frac{dx}{x} = 1 + \ln\frac{t}{\pi d} < \ln t, \tag{54}$$

one has

$$\sum_{1 \leq \gamma \leq t/\pi d} \frac{1}{\pi\gamma} < \frac{\ln t}{\pi}. \tag{55}$$

Similarly,

$$\sum_{\gamma > t/\pi d} \frac{1}{\gamma^2} = \sum_{\gamma = [t/\pi d]+1} \frac{1}{\gamma^2} < \int_{[t/\pi d]}^{\infty} \frac{dx}{x^2} = \frac{1}{[t/\pi d]}. \tag{56}$$

Since

$$\frac{t}{\pi^2 d[t/\pi d]} \leqq \frac{t}{\pi^2 d}, \tag{57}$$

one has

$$\sum_{\gamma > t/\pi d} \frac{t}{\pi^2 \gamma^2 d} \leqq \frac{t}{\pi^2 d} \tag{58}$$

and, hence, (53), (55), and (58) yield

$$\sum_{\gamma=1}^{\infty} \min\left(\frac{1}{\pi\gamma}, \frac{t}{\pi^2\gamma^2 d}\right) < \frac{\ln t}{\pi} + \frac{t}{\pi^2 d}, \qquad t \geqq \pi d. \tag{59}$$

When

$$t < \pi d, \tag{60}$$

one has

$$\sum_{\gamma=1}^{\infty} \min\left(\frac{1}{\pi\gamma}, \frac{t}{\pi^2\gamma^2 d}\right) \leqq \frac{t}{\pi^2 d} \sum_{\gamma=1}^{\infty} \frac{1}{\gamma^2} < \frac{2t}{\pi^2 d}. \tag{61}$$

Hence, using (59) and (61) in (51), one obtains

$$|\omega(\alpha) - \alpha| < \frac{2}{P} \sum_{1 \leqq d \leqq t/\pi} \left(\frac{\ln t}{\pi} + \frac{t}{\pi^2 d}\right) + \frac{2}{P} \sum_{1 \leqq d \leqq m} \frac{2t}{\pi^2 d} + \frac{1}{t}. \tag{62}$$

Thus

$$|\omega(\alpha) - \alpha| < \frac{4}{\pi^2 P} t \ln t + \frac{4t}{\pi^2 P} \sum_{1 \leqq d \leqq m} \frac{1}{d} + \frac{1}{t}. \tag{63}$$

In obtaining (63), the estimate of (54) was used. Since

$$\sum_{1 \leqq d \leqq m} \frac{1}{d} < 1 + \ln m < 2 \ln m, \qquad m \geqq 3,$$

one has

$$|\omega(\alpha) - \alpha| < \frac{4t \ln t + 8t \ln m}{\pi^2 P} + \frac{1}{t}. \tag{64}$$

Let

$$0 < t \leqq m;$$

then

$$|\omega(\alpha) - \alpha| < \frac{12 \ln m}{\pi^2 P} t + \frac{1}{t}. \tag{65}$$

The choice

$$t = \frac{\pi}{2} \sqrt{\frac{P}{3 \ln m}} \tag{66}$$

yields the inequality of the theorem.

When

$$m = 2^\alpha, \qquad \alpha > 2, \tag{67}$$

the period is given by

$$P = \tfrac{1}{2}\phi(m) = 2^{\alpha-2}, \tag{68}$$

and there is no primitive root; hence, Theorem 5 is not directly applicable. The estimation of the trigonometric sum depended on Lemma 5 which requires r to run over a reduced residue system. However, if one considers two distinct λ's, the powers of which together constitute a reduced residue system, then Lemma 5 is again operative and the estimate provided by Theorem 5 is valid. In fact, one need only consider the sequence obtained on setting $\lambda = 5$ in order to obtain one half of the required reduced residue system; the other half is provided by the negatives of the first half.

Bell Telephone Laboratories, Inc.
Whippany, New Jersey

1. Joel N. Franklin, "Deterministic simulation of random processes," *Math. Comp.*, v. 17, 1963, pp. 28–59. MR **26** #7125.

2. G. H. Hardy & E. M. Wright, *An Introduction to the Theory of Numbers*, 3rd ed., Clarendon Press, Oxford, 1954, pp. 234–239. MR **16**, 673.