

NRL Report 7311

Criteria for the Design of
a Uniform Random Number Generator

Laura C. Davis
Radar Analysis Staff

September 9, 1971

Approved for public release; distribution
unlimited

DOCUMENT CONTROL DATA - R & D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY (Corporate author) Naval Research Laboratory Washington, D.C. 20390		2a. REPORT SECURITY CLASSIFICATION Unclassified	
		2b. GROUP	
3. REPORT TITLE Criteria for the Design of a Uniform Random Number Generator			
4. DESCRIPTIVE NOTES (Type of report and inclusive dates) An interim report on a continuing NRL Problem			
5. AUTHOR(S) (First name, middle initial, last name) Laura C. Davis			
6. REPORT DATE September 9, 1971		7a. TOTAL NO. OF PAGES 34	7b. NO. OF REFS 6
8a. CONTRACT OR GRANT NO. NRL Problem B01-07.201		9a. ORIGINATOR'S REPORT NUMBER(S) NRL Report 7311	
b. PROJECT NO. SF 11-141-006		9b. OTHER REPORT NO(S) (Any other numbers that may be assigned this report)	
c.			
d.			
10. DISTRIBUTION STATEMENT Approved for public release, distribution unlimited			
11. SUPPLEMENTARY NOTES		12. SPONSORING MILITARY ACTIVITY Department of the Navy (Naval Ship Systems Command) Washington, D.C. 20360	
13. ABSTRACT <p>This report discusses the problem of generating uniformly distributed random numbers on the computer. The class of linear congruential generators is explored, and a recently discovered defect inherent to these generators is described. Fourier analysis is applied to the output sequence of a linear congruential generator, resulting in the formulation of the spectral test, which is interpreted to measure the severity of the defect mentioned above. Implementation of the spectral test is described. A random number generator is presented in which two linear congruential generators are combined to yield an output sequence with better statistical properties than either single generator. A CDC 3800 Fortran computer program for the random number generator is included in the report.</p>			

14. KEY WORDS	LINK A		LINK B		LINK C	
	ROLE	WT	ROLE	WT	ROLE	WT
Random number generator Uniform random number generator Pseudo-random numbers Linear congruential sequence Computer programs						

CONTENTS

Abstract	ii
Problem Status	ii
Authorization	ii
INTRODUCTION	1
LINEAR CONGRUENTIAL SEQUENCES	2
Maximum Period	2
Potency	2
Parallel Hyperplanes	4
SPECTRAL TEST	6
Finite Fourier Transform	6
Fourier Coefficients for Random Samples	9
Fourier Coefficients for a Linear Congruential Sequence	10
Nonzero Fourier Coefficients and Parallel Hyperplanes	11
APPLICATION OF THE SPECTRAL TEST	13
A RANDOM NUMBER GENERATOR	18
ACKNOWLEDGMENT	18
REFERENCES	19
APPENDIX A—Random Number Generator	20
APPENDIX B—Selection of the Linear Congruential Sequences	21
APPENDIX C—Computer Listings and Sample Output	22

ABSTRACT

This report discusses the problem of generating uniform distributed random numbers on the computer. The class of linear congruential generators is explored, and a recently discovered defect inherent to these generators is described. Fourier analysis is applied to the output sequence of a linear congruential generator, resulting in the formulation of the spectral test, which is interpreted to measure the severity of the defect mentioned above. Implementation of the spectral test is described. A random number generator is presented in which two linear congruential generators are combined to yield an output sequence with better statistical properties than either single generator. A CDC 3800 Fortran computer program for the random number generator is included in the report.

PROBLEM STATUS

This is an interim report on a continuing NRL Problem.

AUTHORIZATION

NRL Problem B01-07.201
Project SF 11-141-006-15335

Manuscript submitted May 25, 1971.

CRITERIA FOR THE DESIGN OF A UNIFORM RANDOM NUMBER GENERATOR

INTRODUCTION

Many computer techniques in applied mathematics and statistics require a source of uniformly distributed random numbers. The problem is to make available on the computer a sequence of numbers which behaves like a series of repeated independent samples from a probability distribution uniform on the unit interval.

The source of these numbers might come from outside the machine; for instance, an apparatus using electrical noise to produce random numbers could be linked to the computer, or a table of previously prepared random numbers could be stored in memory or made available on punched cards or magnetic tape. The first method, however, makes it impossible to repeat calculations exactly, and the second suggestion has restricted usefulness in view of computer storage limitations and input-output time delays.

Alternatively the desired sequences could be generated within the computer using some programmed arithmetic process. Efficient and easily implemented on any machine, this method of producing random numbers has received considerable attention and is used almost exclusively by computing centers today. Consequently many arithmetic generators have appeared, and various statistical tests to rate them on their apparent randomness have been devised. The output sequences of these deterministic processes are sometimes called pseudo-random or quasi-random sequences to emphasize that they are not really random but merely appear to be from a statistical point of view.

By far the most successful arithmetic random-number generators are those based on linear congruential sequences, often referred to as linear congruential generators. This report will discuss the general class of linear congruential random number generators and will point out a recently discovered property of these generators which can have serious effects in Monte Carlo applications. The spectral test, an a priori statistical test for the randomness of the output sequence of a congruential generator based on the Fourier transform of that sequence, will be developed and interpreted to measure the severity of the effects mentioned above. Finally, a random number generator will be presented in which two linear congruential sequences are combined in such a way as to produce an output string with better statistical properties than either sequence used alone.

A CDC 3800 Fortran computer program for the random number generator and a discussion of the linear congruential sequences selected for the generator are given in the appendixes.

LINEAR CONGRUENTIAL SEQUENCES

A linear congruential sequence $\{x_n\}$ is defined by the relation

$$x_{n+1} \equiv ax_n + c \pmod{m}, \quad n \geq 0, \quad (1)$$

where

x_0 is the starting integer value, $x_0 \geq 0$,
 a is called the integer multiplier, $a \geq 0$,
 c is called the integer increment, $c \geq 0$,
 m is the modulus, $m > x_0$, $m > a$, $m > c$.

A sequence in which $c = 0$ is often called multiplicative, and a sequence in which $c \neq 0$ is termed mixed. Any linear congruential sequence must eventually repeat itself, since it contains at most m different values with each element determined solely by its predecessor. Since the period of the sequence cannot exceed the modulus, m should be large; a useful choice is to select m on the order of the computer word size.

Maximum Period

THEOREM 1. *A linear congruential sequence with multiplier a , increment c , and modulus m has maximum period m if and only if:*

- (i) c is relatively prime to m ,
- (ii) $a \equiv 1 \pmod{p}$ if p is a prime factor of m ,
- (iii) $a \equiv 1 \pmod{4}$ if 4 is a factor of m .

A proof of this basic theorem is given by Hull and Dobell⁽¹⁾ among others. If m is a power of 2, then c need only be odd and $a \equiv 1 \pmod{4}$ to insure a maximum period for the sequence.

A maximum period, although obviously desirable and assumed to be the case in the discussion to follow, is not a sufficient condition for randomness; for example the sequence generated by the relation $x_{n+1} = x_n + 1 \pmod{m}$ has period m but can hardly be considered random.

Potency

A second important concept related to the apparent randomness of a linear congruential sequence is that of potency. The potency of a linear congruential sequence of maximum period is defined to be the smallest integer s such that

$$(a - 1)^s \equiv 0 \pmod{m}.$$

THEOREM 2. *The potency of a linear congruential sequence of maximum period m always exists.*

Proof. The integer m can be expressed as the product of a finite number of prime integers:

$$m = \prod_{i=1}^n p_i.$$

By Theorem 1(ii), $a - 1 \equiv 0$ (modulo p) for every prime factor p of m . Thus there exists integers k_i such that

$$a - 1 = k_i p_i, \text{ for } i = 1, \dots, n,$$

or

$$\begin{aligned} (a - 1)^n &= \prod_{i=1}^n k_i p_i \\ &= m \prod_{i=1}^n k_i, \end{aligned}$$

so that $(a - 1)^n \equiv 0$ (modulo m), completing the proof.

If $a = 1$, then

$$x_n \equiv x_{n-1} + c \text{ (modulo } m)$$

or

$$x_n \equiv x_0 + nc \text{ (modulo } m),$$

which is not randomlike behavior. Therefore we may assume $a \geq 2$ and express the n th element in a linear congruential sequence in terms of the starting value as

$$x_n \equiv a^n x_0 + \frac{c(a^n - 1)}{a - 1} \text{ (modulo } m), \text{ for } n \geq 1. \quad (2)$$

This form follows directly from (1) through induction. Since all integers between 0 and $m - 1$ appear somewhere in a sequence with maximum period, we may take $x_0 = 0$ in (2) and expand the factor $a^n - 1 = [(a - 1) + 1]^n - 1$ by the binomial theorem to obtain

$$x_n \equiv c \left[n + \binom{n}{2}(a - 1) + \binom{n}{3}(a - 1)^2 + \dots + \binom{n}{s}(a - 1)^{s-1} \right] \text{ (modulo } m),$$

where s is the potency of the sequence, thereby forcing terms in $a - 1$ of order s or higher to zero. If the potency $s = 1$, then $x_n = nc$ (modulo m), a poor generator of random numbers. If the potency is 2, then

$$x_n \equiv cn + c \binom{n}{2} (a - 1) \pmod{m}$$

and

$$x_{n+1} \equiv c(n + 1) + c \binom{n + 1}{2} (a - 1) \pmod{m},$$

so that

$$x_{n+1} - x_n \equiv c + nc(a - 1) \pmod{m},$$

illustrating the unfortunately simple relation existing between adjacent values of n . The situation improves as the potency becomes larger; Knuth (2) claims on the basis of experience that a potency of at least 5 seems to be required for sufficiently random values from a linear congruential sequence.

THEOREM 3. *A maximum-period linear congruential sequence with multiplier a and modulus $m = 2^n \geq 8$ achieves its greatest potency when $a \equiv 5 \pmod{8}$.*

Proof. By Theorem 1(iii), $a - 1 \equiv 0 \pmod{4}$. If $a - 1$ is an even multiple of 4, then $a - 1 \equiv 0 \pmod{8}$; if $a - 1$ is an odd multiple of 4, then $a - 1 \equiv 4 \pmod{8}$ or equivalently $a \equiv 5 \pmod{8}$. Suppose $a - 1$ is any odd multiple of 4. Then $a - 1 = 4(2k - 1)$ for some integer k . By Theorem 2, $(a - 1)^s \equiv 0 \pmod{2^n}$ for some positive integer s ; therefore 2^n divides $4^s(2k - 1)^s$, which implies 2^n divides 4^s . Hence for any other $a - 1$, say $a - 1 = d$, where d is an even multiple of 4, $d^s \equiv 0 \pmod{2^n}$, proving the theorem.

Parallel Hyperplanes

Marsaglia (3) has pointed out a defect inherent to all multiplicative linear congruential generators. He has shown that if n -tuples (u_1, u_2, \dots, u_n) , $(u_2, u_3, \dots, u_{n+1})$, \dots of successive variates produced by such a generator are considered as points in Euclidean n -space, then all the points will lie in a small number of parallel hyperplanes. In many Monte Carlo applications more than one random number is required at a time, so a periodic structure to the behavior of n -tuples of supposedly uniform random samples could be disastrous. Unfortunately this same effect also appears in the output sequence of the mixed linear congruential generator, as shown below.

Let $\{x_k\}$ be a linear congruential sequence,

$$x_{k+1} \equiv ax_k + c \pmod{m}, \quad k = 0, 1, 2, \dots,$$

and define $\{u_k\}$ to be the scaled sequence

$$u_k = \frac{x_k}{m}, \quad k = 1, 2, 3, \dots$$

Then the n -tuples $(u_k, u_{k+1}, \dots, u_{k+n-1}), (u_{k+1}, u_{k+2}, \dots, u_{k+n}), \dots$, formed from consecutive terms of $\{u_k\}$ may be regarded as points contained in the n -dimensional unit cube. For any set of integers q_1, q_2, \dots, q_n , define

$$q(a) = \sum_{i=1}^n q_i a^{i-1}; \quad h(a) = \sum_{i=2}^n q_i \sum_{j=0}^{i-2} a^j. \quad (3)$$

Note that the following can be obtained from (3):

$$h(a) = \frac{q(a) - q(1)}{a - 1} \text{ for } a \neq 1; \quad h(1) = \lim_{a \rightarrow 1} \frac{q(a) - q(1)}{a - 1}.$$

THEOREM 4. *Let q_1, q_2, \dots, q_n be any set of integers such that*

$$q(a) \equiv 0 \pmod{m}.$$

Then all of the points $(u_k, u_{k+1}, \dots, u_{k+n-1}), (u_{k+1}, u_{k+2}, \dots, u_{k+n}), \dots$ lie in the set of hyperplanes defined by the equations

$$\sum_{i=1}^n q_i t_i = N + \frac{h(a)c}{m}, \quad N = 0, \pm 1, \pm 2, \dots$$

Proof. Using induction on (1), the $(k+r)$ th element of the sequence $\{x_k\}$ may be expressed in terms of the k th element by

$$x_{k+r} \equiv a^r x_k + c \sum_{j=0}^{r-1} a^j \pmod{m} \quad (4)$$

for integers $k \geq 0, r \geq 1$. So

$$\begin{aligned} \sum_{i=1}^n q_i x_{k+i-1} &\equiv \sum_{i=1}^n q_i \left(a^{i-1} x_k + c \sum_{j=0}^{i-2} a^j \right) \pmod{m} \\ &\equiv q(a)x_k + h(a)c \pmod{m} \end{aligned} \quad (5)$$

upon substitution of (4) for all x_ℓ with $\ell > k$. Equivalently (5) may be written without the modulo as

$$\sum_{i=1}^n q_i x_{k+i-1} = jm + q(a)x_k + h(a)c. \quad (6)$$

By the conditions of the theorem, $q(a) \equiv 0 \pmod{m}$; that is, $q(a) = \ell m$ for some integer ℓ . Therefore (6) becomes

$$\sum_{i=1}^n q_i u_{k+i-1} = (j + \ell x_k) + \frac{h(a)c}{m},$$

where each side has also been divided by m . Thus each point $(u_k, u_{k+1}, \dots, u_{k+n-1})$ lies on a hyperplane of the form

$$\sum_{i=1}^n q_i t_i = N + \frac{h(a)c}{m}, \quad N = 0, \pm 1, \pm 2, \dots,$$

and the theorem is proved. Note that $q(a) \equiv 0 \pmod{m}$ always has a nontrivial solution and that the number of hyperplanes intersecting the n -dimensional unit cube cannot exceed $\sum_{i=1}^n |q_i|$.

SPECTRAL TEST

A relative measure of the nonrandomness due to the hyperplane property of linear congruential generators discussed in the last section is the spectral test, which employs a technique proposed by Coveyou and MacPherson (4). This technique involves using Fourier analysis to investigate the statistical independence of successive n -tuples of values produced by these generators. Although the statistical properties of a uniform random number generator are completely characterized by the probability densities of the n -tuples, $n = 1, 2, \dots$, formed from consecutive terms of its output sequence, these densities are usually quite difficult to calculate directly. Since the same information is preserved under a finite Fourier transform, any statistic dependent on the averaging of n consecutive values over the full period of the sequence could theoretically be derived from the transformed density functions. Coveyou and MacPherson point out that the Fourier coefficients themselves are sufficient statistics and are usually fairly simple to calculate. Thus by comparing the Fourier coefficients of the transform of a truly uniform random sequence with those of the transform of a uniform random number generator for given n -tuple sizes, the spectrum of deviations by the generator from uniform randomness is obtained.

Finite Fourier Transform

For a given m define

$$J = \{0, 1, 2, \dots, m-1\}$$

and for $n \geq 2$

$$J_n = \{(j_1, j_2, \dots, j_n) : j_i \in J, i = 1, \dots, n\}.$$

Let $e(w) = \exp(2\pi iw/m)$ for any scalar w . If $x = (x_1, x_2, \dots, x_n)$, define

$$\begin{aligned}\delta(x) &= \delta(x_1, x_2, \dots, x_n) = 1 \text{ if all the } x_i \text{ are integers,} \\ &= 0 \text{ otherwise;}\end{aligned}$$

thus

$$\delta(x_1, x_2, \dots, x_n) = \delta(x_1)\delta(x_2)\dots\delta(x_n).$$

For any integer q

$$\frac{1}{m} \sum_{k=1}^m e(qk) = \delta\left(\frac{q}{m}\right),$$

since if q is divisible by m , then each side is equal to 1 and if q is not divisible by m , then $\delta(q/m) = 0$ by definition and the left side is zero because the summation of a geometric progression gives

$$\begin{aligned}\frac{1}{m} \sum_{k=1}^m [e(q)]^k &= \frac{e(q)}{m} \frac{[1 - e(qm)]}{[1 - e(q)]} \\ &= 0.\end{aligned}$$

Similarly, if $z = (z_1, z_2, \dots, z_n)$ for integers z_i , then

$$\frac{1}{m^n} \sum_{y \in J_n} e(y \cdot z) = \delta\left(\frac{z}{m}\right),$$

where

$$\delta\left(\frac{z}{m}\right) = \prod_{i=1}^n \delta\left(\frac{z_i}{m}\right).$$

THEOREM 5. *If $f(x)$ is any complex function defined on J_n , then it may be represented uniquely by*

$$f(x) = \frac{1}{m^n} \sum_{y \in J_n} e(x \cdot y)g(y), \quad (7)$$

where

$$g(y) = \sum_{z \in J_n} e(-y \cdot z) f(z), \quad (8)$$

the "finite Fourier transform" of $f(x)$.

Proof. For $x \in J_n$

$$\begin{aligned} f(x) &= \sum_{z \in J_n} \delta\left(\frac{x-z}{m}\right) f(z) \\ &= \sum_{z \in J_n} \frac{1}{m^n} \sum_{y \in J_n} e[(x-z) \cdot y] f(z) \\ &= \frac{1}{m^n} \sum_{y \in J_n} e(x \cdot y) \sum_{z \in J_n} e(-y \cdot z) f(z) \\ &= \frac{1}{m^n} \sum_{y \in J_n} e(x \cdot y) g(y). \end{aligned}$$

Suppose $g(y)$ is any function defined on J_n satisfying (7). Then

$$\begin{aligned} g(y) &= \sum_{z \in J_n} \delta\left(\frac{z-y}{m}\right) g(z) \\ &= \sum_{z \in J_n} \frac{1}{m^n} \sum_{x \in J_n} e[(z-y) \cdot x] g(z) \\ &= \sum_{x \in J_n} e(-x \cdot y) \frac{1}{m^n} \sum_{z \in J_n} e(x \cdot z) g(z) \\ &= \sum_{x \in J_n} e(-x \cdot y) f(x), \end{aligned}$$

and $g(y)$, the finite Fourier transform of $f(x)$ as defined in (8), is unique, concluding the proof. Note that $e(w) = e(v)$ if and only if $w \equiv v$ (modulo m), so that $g(y)$ is a periodic function.

Let $\{x_k\}$ be a sequence of elements of J and $\{y_k\}$ a sequence of elements of J_n such that $y_k = (x_k, x_{k+1}, \dots, x_{k+n-1})$. Then for $z \in J_n$ define $f(z)$ to be the limit as N approaches

infinity of the proportion of appearances of z in the first N terms of the sequence $\{x_k\}$, assuming this limit exists. That is,

$$f(z) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{k=0}^{N-1} \delta\left(\frac{z - y_k}{m}\right).$$

In addition, for $r \in J_n$ define

$$\varphi(r) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{k=0}^{N-1} e(-r \cdot y_k), \quad (9)$$

so that, assuming the limit exists,

$$\varphi(r) = \sum_{z \in J_n} e(-r \cdot z) f(z). \quad (10)$$

The right side of (10) is in the form of (8), the finite Fourier transform of f , so by (7) we have

$$f(z) = \frac{1}{m^n} \sum_{r \in J_n} e(z \cdot r) \varphi(r). \quad (11)$$

If $\{x_k\}$ is actually the output sequence of an arithmetic generator and $f(z)$ as defined above exists for each $z \in J_n$, then $f(z)$ is the joint density function of n consecutive terms of the sequence $\{x_k\}$.

Fourier Coefficients for Random Samples

If the sequence $\{x_k\}$ consisted of truly random samples from a uniform distribution on the integers in J , then each element of J_n would appear equally often in the sequence $\{y_k\}$, so that $f(z) = 1/m^n$, for all $z \in J_n$. From (11) we have

$$f(z) = \frac{1}{m^n} \sum_{r \in J_n} e(z \cdot r) \varphi(r), \quad z \in J_n,$$

so that the finite Fourier coefficients must take the values

$$\begin{aligned} \varphi(r) &= 1 \text{ when all } r_i \equiv 0 \text{ (modulo } m), \quad 1 \leq i \leq n, \\ &= 0 \text{ otherwise.} \end{aligned}$$

Fourier Coefficients for a Linear Congruential Sequence

Let $\{x_k\}$ be a linear congruential sequence of maximum period, where $x_{k+1} \equiv ax_k + c$ (modulo m). By (9) the finite Fourier transform of the joint density function of n consecutive terms of the sequence $\{x_k\}$ has the form

$$\varphi(q) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{k=0}^{N-1} e\left(-\left(q_1 x_k + \dots + q_n x_{k+n-1}\right)\right),$$

where $q = (q_1, q_2, \dots, q_n) \in J_n$. Since $\{x_k\}$ is periodic with period m , this limit exists and the Fourier coefficients become

$$\varphi(q) = \frac{1}{m} \sum_{k=0}^{m-1} e\left(-\left(q_1 x_k + \dots + q_n x_{k+n-1}\right)\right). \quad (12)$$

Recall from (4) that for any linear congruential sequence $x_{k+1} \equiv ax_k + c$ (modulo m), x_{k+r} may be expressed directly in terms of x_k by the relation

$$x_{k+r} \equiv a^r x_k + c \sum_{i=0}^{r-1} a^i \pmod{m} \text{ for } r = 0, 1, 2, \dots \quad (13)$$

Substituting (13) in (12) gives

$$\varphi(q) = \frac{1}{m} \sum_{k=0}^{m-1} e\left(-[q(a)x_k + h(a)c]\right),$$

where $q(a)$ and $h(a)$ are defined by (3). Since $\{x_k\}$ has maximum period, x_k assumes all integer values between 0 and $m-1$, so that

$$\varphi(q) = \frac{1}{m} \sum_{k=0}^{m-1} e\left(-[q(a)k + h(a)c]\right)$$

or

$$\varphi(q) = e(-h(a)c) \frac{1}{m} \sum_{k=0}^{m-1} e(-q(a)k).$$

If $q(a)$ is divisible by m , then

$$\begin{aligned} \frac{1}{m} \sum_{k=0}^{m-1} e(-q(a)k) &= \frac{1}{m} \sum_{k=0}^{m-1} 1^k \\ &= 1. \end{aligned}$$

If $q(a)$ is not divisible by m , then by the sum of a geometric progression

$$\begin{aligned} \frac{1}{m} \sum_{k=0}^{m-1} e^{-q(a)k} &= \frac{1}{m} \sum_{k=0}^{m-1} e^{-q(a)k} \\ &= \frac{1}{m} \frac{[1 - e^{-q(a)m}]}{[1 - e^{-q(a)}]} \\ &= 0. \end{aligned}$$

Therefore the Fourier coefficients take the form

$$\varphi(q) = e^{-h(a)c} \delta\left(\frac{q(a)}{m}\right), \quad (14)$$

where δ was defined earlier as

$$\begin{aligned} \delta\left(\frac{q(a)}{m}\right) &= 1 \text{ if } \frac{q(a)}{m} \text{ is an integer,} \\ &= 0 \text{ otherwise.} \end{aligned}$$

Note that $\varphi(q) = 0$ except when $q(a)$ is divisible by m ; that is, $\varphi(q) \neq 0$ if and only if $q(a) \equiv 0$ (modulo m), and then $|\varphi(q)| = 1$.

In the preceding subsection it was shown that if the sequence $\{x_k\}$ were a set of random samples from a uniform distribution on the integers $J = \{0, 1, \dots, m-1\}$, then

$$\begin{aligned} |\varphi(q)| &= 1 \text{ if } q_i \equiv 0 \text{ (modulo } m) \text{ for all } 1 \leq i \leq n, \\ &= 0 \text{ otherwise.} \end{aligned}$$

Thus the nonzero Fourier coefficients of a linear congruential sequence represent deviations of the sequence from true randomness and are characterized by the solutions to the basic congruence

$$q_1 + q_2 a + q_3 a^2 + \dots + q_n a^{n-1} \equiv 0 \text{ (modulo } m),$$

where the q_i are not all zero.

Nonzero Fourier Coefficients and Parallel Hyperplanes

By Theorem 4 it was shown that if q_1, q_2, \dots, q_n were any set of integers such that

$$q_1 + q_2 a + q_3 a^2 + \dots + q_n a^{n-1} \equiv 0 \text{ (modulo } m),$$

then all the points $(x_1/m, x_2/m, \dots, x_n/m), (x_2/m, x_3/m, \dots, x_{n+1}/m) \dots$ lie on one of the parallel hyperplanes defined by the equation

$$q_1 t_1 + q_2 t_2 + \dots + q_n t_n = N + \frac{h(a)c}{m}, \quad (15)$$

where N ranges over the integers and $h(a)$ is defined by (3). Hence each $q = (q_1, q_2, \dots, q_n) \in J_n$, such that the Fourier coefficient $\varphi(q)$ discussed above is nonzero, defines a set of parallel hyperplanes in Euclidean n -space containing all the n -tuples $(x_k/m, x_{k+1}/m, \dots, x_{k+n-1}/m)$, $k \geq 1$, treated as points in the n -dimensional unit cube.

The distance between two neighboring planes can be calculated by considering the related families of parallel hyperplanes

$$q_1 t_1 + q_2 t_2 + \dots + q_n t_n = N, \quad N = 0, \pm 1, \pm 2, \dots,$$

which is just (15) shifted so that the plane defined by $N = 0$ passes through the origin. Obviously the planes are equidistant, and if $Q = (q_1, q_2, \dots, q_n)$ and $T = (t_1, t_2, \dots, t_n)$, then the planes may be written in the form

$$Q \cdot T = N, \quad N = 0, \pm 1, \pm 2, \dots$$

The distance d between two adjacent planes is the length of the vector from the origin normal to the plane $Q \cdot T = 1$, so that

$$d = \frac{1}{|Q|}$$

or

$$d = (q_1^2 + q_2^2 + \dots + q_n^2)^{-1/2}.$$

Define $P_a = \{Q = (q_1, q_2, \dots, q_n): 0 \leq q_i < m \text{ not all zero for } 1 \leq i \leq n \text{ and } q(a) \equiv 0 \pmod{m}\}$. For a given m and n , P_a represents the collection of hyperplane families for a particular multiplier a , each family containing all the points $(x_k/m, x_{k+1}/m, \dots, x_{k+n-1}/m)$, $k = 1, 2, \dots$. Each such collection can be characterized by its "worst possible case": that family or families of hyperplanes whose interplane distance is the greatest. Actually this distance itself is of interest, and since the distance between adjacent planes in any family is $1/|Q|$, define

$$\gamma_n = \min_{Q \in P_a} |Q|,$$

so that

$$\frac{1}{\gamma_n} \geq \frac{1}{|Q|} \text{ for } Q \in P_a.$$

Since the sequence $\{x_k\}$ has a finite period of length m , there exists a $Q \in P_a$ such that

$$\frac{1}{\gamma_n} = \frac{1}{|Q|}.$$

The larger the value of γ_n , the smaller the distance between adjacent planes in even the most widely spaced hyperplane family and the more homogeneous the n -tuples $(x_k/m, x_{k+1}/m, \dots, x_{k+n-1}/m)$, $k = 1, 2, \dots$, considered as points in n -dimensional space. Thus γ_n can be used as an indication of randomness for a particular linear congruential sequence in regard to the uniformity of the distribution of its n -tuples.

Unfortunately γ_n cannot be made arbitrarily large by the proper choice of the multiplier a in the linear congruential sequence (γ_n is independent of the increment c). It can be shown that

$$\gamma_n \leq \beta_n m^{1/n},$$

where β_n takes on the values $1, (4/3)^{1/4}, 2^{1/6}, 2^{1/4}, 2^{3/10}, (64/3)^{1/12}, 2^{3/7}, 2^{1/2}$, for $n = 1, 2, \dots, 8$ respectively. (See Knuth (2), pp. 85-86, and his references.) So a reasonable figure of merit may be defined to be the ratio $\gamma_n/\beta_n m^{1/n}$, where unity is the best that can be achieved.

APPLICATION OF THE SPECTRAL TEST

To calculate the ratio $\gamma_n/\beta_n m^{1/n}$ for a particular linear congruential sequence, characterized here by its multiplier a for a fixed m and n , the minimum value of the quantity $(q_1^2 + q_2^2 + \dots + q_n^2)^{1/2}$ must be determined, where the integers $0 \leq q_i < m$ are not all zero and satisfy the congruence relation

$$q_1 + aq_2 + a^2q_3 + \dots + a^{n-1}q_n \equiv 0 \pmod{m}.$$

Let $\alpha_i \equiv a^i \pmod{m}$, for $i = 1, \dots, n-1$. Then the problem is equivalent to finding the minimum value of

$$(v_1 m - \alpha_1 v_2 - \alpha_2 v_3 - \dots - \alpha_{n-1} v_n)^2 + v_2^2 + \dots + v_n^2 \quad (16)$$

for integers v_1, v_2, \dots, v_n not all zero.

Define V to be the set of all n -dimensional column vectors,

$$v = \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix},$$

with integer components not all zero. Then (16) may be rewritten as $v^T(A^T A)v$, for $v \in V$ and

$$A = \begin{pmatrix} m & -\alpha_1 & -\alpha_2 & \dots & -\alpha_{n-1} \\ 0 & 1 & 0 & \dots & 0 \\ \dots & \dots & 1 & \dots & \dots \\ \dots & \dots & \dots & \dots & 0 \\ 0 & \dots & \dots & 0 & 1 \end{pmatrix}.$$

The matrix A consists of integer elements, and $\det(A) = m$.

Based on the work of Coveyou and MacPherson (3), Knuth has developed a computational method for solving a more general problem than the one posed above. (The method outlined here is essentially a more rigorous version of Knuth (2), pp. 89-93.) Let A be an n -by- n nonsingular matrix composed of integer elements, and define

$$G(A) = \{v^T(A^T A)v : v \in V\}.$$

Since $A^T A$ is positive definite and all elements of A are integers, $G(A)$ is a nonempty set of positive integers and therefore contains a least member. The problem, then, is to determine γ^2 , where

$$\gamma^2 = \min G(A).$$

Let

$$W = \{v \in V : v^T(A^T A)v = \gamma^2\}.$$

For simplicity define $Q = A^T A$, $R = Q^{-1}$, and $B = A^{-1}$. If E is an arbitrary matrix, let E_i represent the i th row of E and $E_{.j}$ represent the j th column of E .

THEOREM 6. *If $w \in W$ and $v \in V$, then $w_k^2 \leq R_{kk}(v^T Q v)$ for $k = 1, 2, \dots, n$.*

Proof. Let $e_k \in V$ be the vector which is zero except for 1 in the k th component. Then

$$w_k = e_k^T w = e_k^T (BA)w = (e_k^T B)(Aw) = (B_k)(Aw)$$

and

$$\begin{aligned} [(B_k)(Aw)]^2 &\leq [(B_k)(B_k)] [(Aw)(Aw)] = [(B_k)(B_k^T)] [w^T(A^T A)w] \\ &= R_{kk} w^T Q w \end{aligned}$$

by the Schwarz inequality. Thus for vectors w and v

$$w_k^2 \leq R_{kk}(w^T Q w) \leq R_{kk}(v^T Q v),$$

concluding the proof.

COROLLARY. If $w \in W$, then $w_k^2 \leq R_{kk} Q_{jj}$, $1 \leq k \leq n$, $1 \leq j \leq n$.

Proof. The proof follows directly from Theorem 6 with $v = e_j$.

Consequently,

$$W \subseteq Y = \prod_{k=1}^n \left(-\left\lfloor (R_{kk} Q_{jj})^{1/2} \right\rfloor, \dots, \left\lfloor (R_{kk} Q_{jj})^{1/2} \right\rfloor \right), \quad (17)$$

where \times indicates the Cartesian product. Since an exhaustive search of the finite set Y would yield all the vectors of W , the number of elements in Y , given by

$$N = \prod_{k=1}^n \left(2 \left\lfloor (R_{kk} Q_{jj})^{1/2} \right\rfloor + 1 \right), \quad (18)$$

bounds the number of vectors to be examined to determine γ^2 . The size of N , however, may be much too large to implement a direct search for a minimum vector, so a succession of integer transformations are applied to the matrix A to reduce the values of the diagonals of matrices Q and R until (17) indicates a search is feasible.

Let \mathcal{U} be the set of all n -by- n matrices of the form

$$(U)_{ij} = \delta_{ij} + c_j \delta_{ik},$$

where k is a positive integer not exceeding n , c_j is an arbitrary integer for $j \neq k$, $c_k = 0$, and

$$\begin{aligned} \delta_{ij} &= 1 \text{ if } i = j, \\ &= 0 \text{ otherwise.} \end{aligned}$$

Then it follows directly that:

- (i) $(U^{-1})_{ij} = \delta_{ij} - c_j \delta_{ik}$, and so \mathcal{U} is closed under inverses.
- (ii) If x is an integer vector and $U \in \mathcal{U}$ then Ux is an integer vector.

Consequently any member of \mathcal{U} maps the integer vectors one-to-one onto the integer vectors. Therefore

$$G(AU^{-1}) = G(A),$$

so that

$$\gamma^2 = \min G(A) = \min G(AU^{-1}).$$

Define $A' = AU^{-1}$, $B' = UB$, $Q' = (U^{-1})^TQU^{-1}$, and $R' = URUT$, for $U \in \mathcal{U}$. The objective here is to select a transformation $U \in \mathcal{U}$ which makes the diagonals of Q' and R' as small as possible and thereby reduces the number of vectors to be examined in (17). From the definitions

$$Q'_{jj} = (A'_{\cdot j}) \cdot (A'_{\cdot j}),$$

and direct computation gives

$$A'_{\cdot j} = A_{\cdot j} - c_j A_{\cdot k},$$

where, since $c_k = 0$,

$$A'_{\cdot k} = A_{\cdot k}.$$

Therefore

$$\begin{aligned} Q'_{jj} &= (A_{\cdot j} - c_j A_{\cdot k}) \cdot (A_{\cdot j} - c_j A_{\cdot k}) \\ &= (A_{\cdot j} \cdot A_{\cdot j}) - 2c_j (A_{\cdot j} \cdot A_{\cdot k}) + c_j^2 (A_{\cdot k} \cdot A_{\cdot k}) \\ &= Q_{jj} - 2c_j Q_{jk} + c_j^2 Q_{kk} \\ &= Q_{kk} \left(c_j - \frac{Q_{jk}}{Q_{kk}} \right)^2 + Q_{jj} - \frac{Q_{jk}^2}{Q_{kk}}, \end{aligned} \quad (19)$$

whose minimum value for $j \neq k$ occurs when

$$c_j = \frac{Q_{jk}}{Q_{kk}}. \quad (20)$$

In the case of the matrix R'

$$R'_{ii} = (B'_{i \cdot}) \cdot (B'_{i \cdot}),$$

and a simple computation shows

$$B'_{i \cdot} = B_{i \cdot} + \delta_{ik} \sum_{j=1}^n c_j B_{j \cdot}.$$

So $R'_{ii} = R_{ii}$ for $i \neq k$, and

$$\begin{aligned} R'_{kk} &= (B_{k \cdot} + \sum_{j=1}^n c_j B_{j \cdot}) \cdot (B_{k \cdot} + \sum_{j=1}^n c_j B_{j \cdot}) \\ &= R_{kk} + 2 \sum_{j=1}^n c_j R_{kj} + \sum_{i=1}^n \sum_{j=1}^n c_i c_j R_{ij}. \end{aligned}$$

Since

$$\frac{\partial R'_{kk}}{\partial c_\ell} = 2R_{k\ell} + 2 \sum_{i=1}^n c_i R_{i\ell}, \text{ for } 1 \leq \ell \leq n, \ell \neq k,$$

the c_i should satisfy the equations

$$R_{k\ell} + \sum_{i=1}^n c_i R_{i\ell} = 0 \text{ for } 1 \leq \ell \leq n, \ell \neq k \quad (21)$$

in order to minimize the diagonal element R'_{kk} .

For a given k , two sets of conditions on the transformation matrix components c_i , $1 \leq i \leq n, i \neq k$, have been derived; the first set, (20), produces a matrix U which minimizes the diagonal elements Q'_{ii} , $1 \leq i \leq n, i \neq k$, and the second, (21), determines a transformation which reduces the diagonal element R'_{kk} . Fortunately (20) and (21) are compatible, as the following theorem shows.

THEOREM 7. *Let k be a positive integer not exceeding n . Then choosing*

$$c_i = \frac{Q_{ik}}{Q_{kk}}, \text{ for } 1 \leq i \leq n, i \neq k,$$

will satisfy the equations

$$R_{kj} + \sum_{i \neq k} c_i R_{ij} = 0, \quad 1 \leq j \leq n, j \neq k.$$

Proof: For $j \neq k$

$$\begin{aligned} Q_{kk} \left[R_{kj} + \sum_{i=1}^n c_i R_{ij} \right] &= Q_{kk} R_{kj} + \sum_{i \neq k} Q_{ik} R_{ij} \\ &= \sum_{i=1}^n Q_{ik} R_{ij} \\ &= (Q \cdot_k) \cdot (R \cdot_j) \\ &= (Q \cdot_k) \cdot (Q \cdot_j^{-1}). \end{aligned}$$

Since $Q = A^T A$ is symmetric,

$$\begin{aligned} (Q_{\cdot k}) \cdot (Q_{\cdot j}^{-1}) &= (Q_{k \cdot}) \cdot (Q_{\cdot j}^{-1}) \\ &= 0, \end{aligned}$$

proving the theorem.

The c_j must be integers, so taking the integer nearest to Q_{jk}/Q_{kk} for each $1 \leq j \leq n$, $j \neq k$, gives the best integer solution to (19) and close to (but not always equal to) the best integer solution to (21). Therefore it is plausible that repeated transformations of Q and R by matrices of the form

$$(U)_{ij} = \delta_{ij} + c_j \delta_{ik}$$

for different choices of k with the c_j determined as above will give a value for N in (18) small enough to make an exhaustive search for the minimizing vector reasonable. No proof is available that this scheme always terminates, but in practice no difficulties have been encountered and the method has proven quite efficient.

A RANDOM NUMBER GENERATOR

The spectral theory developed earlier offers a powerful test for the randomness of linear congruential generators by considering the distribution of n -tuples, $(x_k, x_{k+1}, \dots, x_{k+n-1})$, $k = 1, 2, \dots$, of the output sequence $\{x_k\}$.

It has been pointed out, however, that the confinement to parallel hyperplanes of successive n -tuples of variates produced by a linear congruential sequence cannot be completely removed by adjusting the sequence parameters. In light of this problem, a procedure first suggested by MacLaren and Marsaglia (5) is advocated. Two linear congruential generators are required, one to shuffle the sequence produced by the other. The method works as follows: the first generator initially fills a table with random numbers; whenever a random number is needed, the second generator determines which entry in the table is selected; the first generator then supplies a replacement in the table. Tests applied by MacLaren and Marsaglia, and later by Gebhardt (6) on a special case using Fibonacci sequences, show this scheme to have better statistical properties than either of the two congruential generators used alone. Thus a reliable random number generator can be constructed by selecting two linear congruential sequences with maximum period, high potency, and minimum distance between hyperplanes and employing them in the above manner. Although it may take twice as long to produce a sequence of random numbers using two congruential generators rather than one, the additional time seems well spent in order to obliterate the hyperplane structure inherent to the single congruential generator. A particular random number generator employing this method is described in the Appendixes.

ACKNOWLEDGMENT

The author expresses her appreciation to Mr. David J. Kaplan of NRL for valuable discussions and helpful suggestions concerning this work.

REFERENCES

1. Hull, T.E., and Dobell, A.R., "Random Number Generators," SIAM Review 4(3): 230-254 (July 1962).
2. Knuth, D.E., "The Art of Computer Programming: Seminumerical Algorithms," Addison-Wesley, 1969.
3. Marsaglia, G., "Random Numbers Fall Mainly in the Planes," Proc. N.A.S. 61: 25-28 (1968).
4. Coveyou, R.R., and MacPherson, R.D., "Fourier Analysis of Uniform Random Number Generators," JACM 14(1): 100-119 (Jan. 1967).
5. MacLaren, M.D., and Marsaglia, G., "Uniform Random Number Generators," JACM 12(1): 83-89 (Jan. 1965).
6. Gebhardt, F., "Generating Pseudo-Random Numbers by Shuffling a Fibonacci Sequence," Math. Comp. 21(100): 708-709 (Oct. 1967).

APPENDIX A RANDOM NUMBER GENERATOR

The uniform random number generator presented here employs two linear congruential sequences $\{x_n\}$ and $\{y_n\}$, where

$$x_{n+1} \equiv a_1 x_n + c_1 \pmod{m}, \quad n = 0, 1, 2, \dots,$$

$$y_{n+1} \equiv a_2 y_n + c_2 \pmod{m}, \quad n = 0, 1, 2, \dots$$

Given a starting value x_0 , an array is filled with the first 64 values of $\{x_n\}$. Whenever a random number is required, the current value in the sequence $\{y_n\}$ determines which entry in the array is selected. The number chosen is then replaced in the array with the current value in the sequence $\{x_n\}$.

The generator package consists of three routines. Subroutine RANSET initializes the linear congruential sequences $\{x_n\}$ and $\{y_n\}$ and sets up the random number array mentioned above. Subroutine RANSET must be called once within a program, prior to any reference to the other two routines. Function RAND returns either a floating-point random number from the unit interval or a fixed-point random integer from a specified set of positive integers, depending on the value of its single parameter. Subroutine RANOUT produces the contents of the 64-word random number array and the current value in each of the sequences $\{x_n\}$ and $\{y_n\}$ as output on punched cards. These cards may then be read by subroutine RANSET at the beginning of a subsequent run to resume random number generation from this point. Details on the calling procedure and operation of each routine are explained in the program listing in Appendix C. A test program using the random-number package and a sample output are included.

The routines are written in ANSI X3.9-1966 Standard Fortran, with the exception of the data statement format appearing in subroutine RANSET, which is apparently unique to CDC 3600-3800 Fortran. The only library function called by the package is MOD, the modulo function. The three machine-dependent variables are noted in the program listing. Trial runs of the Fortran program were made on a CDC 3800 computer, and the time to obtain a single floating-point random number averaged 190 microseconds.

**APPENDIX B
SELECTION OF THE LINEAR CONGRUENTIAL SEQUENCES**

The parameters of the linear congruential sequences $\{x_n\}$ and $\{y_n\}$ used by the random number generator were determined as follows. The modulo m for both sequences was taken to be 2^{31} , so that the generator may be run on any computer whose word length exceeds 32 bits. The increments c_1 and c_2 were chosen such that

$$\frac{c_i}{m} \approx \frac{1}{2} - \frac{\sqrt{3}}{6}, \quad i = 1, 2,$$

in order to minimize serial correlation, as discussed by Knuth* and were made odd to ensure maximum period by Theorem 1. The multipliers a_1 and a_2 were required to satisfy

$$a_i \equiv 5 \pmod{8}, \quad i = 1, 2, \tag{B1}$$

for maximum period and high potency by Theorems 1 and 3 and also to satisfy

$$\frac{m}{100} < a_i < m - \sqrt{m}, \quad i = 1, 2, \tag{B2}$$

as recommended by Knuth in his summary on random numbers, since small multipliers tend to produce poor sequences. A candidate multiplier that satisfied conditions (B1) and (B2) was subjected to the spectral test for $n = 2, 3, 4, 5, 6$. The ratio $\gamma_n/\beta_n m^{1/n}$ was calculated for each n , and the potential multiplier was rejected if the ratio fell below the arbitrary threshold of 0.6 for any n . In a run of over 100 candidates, two multipliers met the above criteria and were selected as a_1 and a_2 for the linear congruential sequences $\{x_n\}$ and $\{y_n\}$. The two linear congruential sequences used in the random number generator are

$$x_{n+1} = 504542181 x_n + 453816693 \pmod{2^{31}}$$

$$y_{n+1} = 266891877 y_n + 453816697 \pmod{2^{31}}.$$

*D.E. Knuth, "The Art of Computer Programming: Seminumerical Algorithms," Addison-Wesley, 1969, pp. 77-78.

FUNCTION RAND(N)

AUTHOR

LAURA DAVIS, NRL, CODE 5308

DATE OF LAST REVISION

OCTOBER 23, 1970

WRITTEN IN USA STANDARD FORTRAN

DESCRIPTION

THE PURPOSE OF RAND IS TO GENERATE A SEQUENCE OF UNIFORMLY DISTRIBUTED RANDOM NUMBERS. A MIXED LINEAR CONGRUENTIAL SEQUENCE X , $X(I+1) = A1 * X(I) + C1 \text{ (MODULO } M)$, IS USED TO SUPPLY INITIAL VALUES TO A 64 WORD AUXILIARY RANDOM NUMBER TABLE (SEE SUBROUTINE RANSET). WHEN RAND IS CALLED, THE 6 HIGH ORDER BITS OF THE CURRENT VALUE IN A SECOND LINEAR CONGRUENTIAL SEQUENCE Y , $Y(I+1) = A2 * Y(I) + C2 \text{ (MODULO } M)$, ARE EXTRACTED AS AN INDEX TO SELECT A NUMBER FROM THE TABLE. THE LOCATION USED IS THEN REFILLED WITH THE NEXT NUMBER GENERATED BY THE X CONGRUENTIAL SEQUENCE.

USAGE

NOTE -- THE RANDOM NUMBER GENERATOR INITIALIZATION SUBROUTINE RANSET MUST BE CALLED ONCE WITHIN A PROGRAM PRIOR TO ANY REFERENCES TO RAND,

$Z = \text{RAND}(N)$

N.LE.0 RAND RETURNS A FLOATING POINT RANDOM NUMBER UNIFORMLY DISTRIBUTED ON THE UNIT INTERVAL.

N.GT.1 RAND RETURNS A FIXED POINT RANDOM INTEGER UNIFORMLY DISTRIBUTED ON THE CLOSED INTERVAL (1,N).

CAUTION -- SINCE RAND IS A TYPE REAL FUNCTION, THE RANDOM INTEGER RETURNED ABOVE SHOULD BE HANDLED AS FOLLOWS

- 1) EQUIVALENCE (Z,IZ) IN THE CALLING PROGRAM
- 2) LET $Z = \text{RAND}(N)$, N.GT.1
- 3) USE IZ TO REFERENCE THE RANDOM INTEGER

FUNCTIONS OR SUBROUTINES REQUIRED

MOD --- AN INTEGER MODULO FUNCTION

COMMON/RANDOM/M,FP,IM,IW,IX,A1,C1,IY,A2,C2,IR(64)

INTEGER A1, C1, A2, C2

EQUIVALENCE (WS, IWS)

CALCULATE TABLE INDEX USING LINEAR CONGRUENTIAL SEQUENCE Y

IY = A2 * IY

IF (IY.LT.0) IY = IY + IW

IY = (IY - M) + C2

```
      IF(IY.LT,0) IY = IY + M
C      USE FIRST SIX BITS OF IY FOR INDEX K
15  IY = MOD(IY,M)
      K = IY/IM + 1
C      EXTRACT RANDOM NUMBER FROM TABLE
      RAND = IR(K)/FM
C      CALCULATE TABLE REPLACEMENT USING CONGRUENTIAL SEQUENCE X
      IX = A1*IX
      IF(IX.LT,0) IX = IX + IW
      IX = (IX - M) + C1
      IF(IX.LT,0) IX = IX + M
C      TAKE IX MODULO M
25  IX = MOD(IX,M)
      IR(K) = IX
      IF (N.LE,0) RETURN
C      RETURN A (1,N) RANDOM INTEGER IN RAND.
      IWS = N*RAND + 1.0
      RAND = WS
      RETURN
      END
```

SUBROUTINE RANSET(I,J,K)

ALTHOUGH
LAURA DAVIS, NRL, CODE 5308

DATE OF LAST REVISION
OCTOBER 23, 1970

WRITTEN IN USA STANDARD FORTRAN EXCEPT FOR THE FORM OF THE DATA STATEMENT

DESCRIPTION
THE PURPOSE OF RANSET IS TO INITIALIZE THE LINEAR CONGRUENTIAL SEQUENCES X AND Y AND SET UP THE AUXILIARY RANDOM NUMBER TABLE USED BY RAND TO OBTAIN A SEQUENCE OF UNIFORMLY DISTRIBUTED RANDOM NUMBERS.

USAGE
NOTE -- RANSET MUST BE CALLED ONCE WITHIN A PROGRAM PRIOR TO ANY REFERENCES TO RAND.

CALL SUBROUTINE RANSET(I,J,K)

K,GE.0

I ---- THE INTEGER STARTING VALUE FOR THE SEQUENCE X,
 $X(I+1) = A1 * X(I) + C1 \pmod{M}$, USED TO CALCULATE
THE INITIAL RANDOM NUMBER TABLE ENTRIES AND
SUBSEQUENT REPLACEMENT VALUES,
J ---- THE INTEGER STARTING VALUE FOR THE SEQUENCE Y,
 $Y(I+1) = A2 * Y(I) + C2 \pmod{M}$, USED BY RAND TO
OBTAIN AN INDEX TO THE RANDOM NUMBER TABLE,

K,LT.0

I ---- IGNORED
J ---- IGNORED
RANSET WILL READ IN VALUES FROM PUNCHED CARDS TO INITIALIZE
THE X AND Y CONGRUENTIAL SEQUENCES AND FILL THE AUXILIARY
RANDOM NUMBER TABLE. THESE INPUT CARDS ARE USUALLY OBTAINED
AS OUTPUT FROM SUBROUTINE RANOUT AT THE END OF AN EARLIER
RUN.

FUNCTIONS OR SUBROUTINES REQUIRED
MOD -- AN INTEGER MODULO FUNCTION

MACHINE DEPENDENT VARIABLES
IK ---- THE LARGEST INTEGER THE MACHINE WILL HOLD
INTAPE - THE STANDARD INPUT LOGICAL UNIT NUMBER

```

COMMON/RANDOM/M,FM,IM,IW,IX,A1,C1,IY,A2,C2,IR(64)
INTEGER A1, C1, A2, C2
DATA      (M=2147483648), (A1=504542181), (C1=453816693)
DATA      (A2=266891877), (C2=453816697)
C      IW = 2**47 - 1 IS USED TO CORRECT A POSITIVE PRODUCT FROM THE QA REGISTER
C      WHICH APPEARS NEGATIVE WHEN STORED DUE TO A BIT IN THE SIGN POSITION OF A
DATA (IW = 140737488355327)
DATA (INTAPE = 60)
FM = M
IM = M/64
IF (K) 50, 10, 10
C      INITIALIZE LINEAR CONGRUENTIAL SEQUENCES X AND Y WITH PARAMETER VALUES
10 IX = I
   IY = J
C      GENERATE 64 RANDOM NUMBERS USING LCS1 AND STORE IN IR
DO 35 L = 1,64
   IX = A1*IX
   IF (IX.LT,0) IX = IX + IW
   IX = (IX - M) + C1
   IF (IX.LT,0) IX = IX + M
C      TAKE X MODULO M
30 IX = MOD (IX,M)
35 IR(L) = IX
   RETURN
C      READ IN CURRENT SEQUENCE VALUES AND RANDOM NUMBER TABLE FROM CARDS
C      PUNCHED PREVIOUSLY BY SUBROUTINE RANDUT
50 READ (INTAPE, 55) IX, IY, (IR(L), L=1,64)
55 FORMAT(2I16/(5I16))
   RETURN
END

```

NEXT 100 RANDOM INTEGERS ON THE CLOSED INTERVAL (1,100) PRODUCED BY RAN

66	1	91	75
73	7	22	84
70	73	36	96
52	10	12	31
39	23	66	15
95	39	46	65
63	91	52	84
59	33	94	84
52	75	36	11
28	28	97	56
52	97	1	84
37	35	3	41
2	34	58	19
71	90	22	32
51	18	94	36
76	39	50	17
94	50	100	25
98	8	11	22
47	45	87	86
40	37	86	41