1976-06

Theory and testing of uniform random number generators

Learmonth, Gerard Paul

Monterey, California. Naval Postgraduate School

THEORY AND TESTING OF UNIFORM RANDOM NUMBER GENERATORS

Gerard Paul Learmonth

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

THEORY AND TESTING OF UNIFORM
RANDOM NUMBER GENERATORS

by

Gerard Paul Learmonth

June 1976

Thesis Advisor: P.A.W. Lewis

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Theory and Testing of Uniform Random Number Generators		5. TYPE OF REPORT & PERIOD COVERED Master's Thesis; June 1976 6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Gerard Paul Learmonth		8. CONTRACT OR GRANT NUMBER(s)
9. PERFORMING ORGANIZATION NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS Naval Postgraduate School Monterey, California 93940		12. REPORT DATE June 1976 13. NUMBER OF PAGES 60
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

Approved for public release; distribution limited.

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Uniform Random Number Generators

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

Two structural tests for random number generators of the Lehmer congruential type are discussed. They are known now to be essentially equivalent but are

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE
S/N 0102-014-6601 |
(Page 1)

UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

(20. ABSTRACT Continued)

formulated incorrectly and the computational algorithms to implement the tests are unnecessarily complicated. New algorithms for these tests will be sketched.

Theory and Testing of Uniform Random Number Generators

by

Gerard Paul Learmonth
B.S., New York University, 1966

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN OPERATIONS RESEARCH

from the

NAVAL POSTGRADUATE SCHOOL

June 1976

ABSTRACT

Two structural tests for random number generators of the Lehmer congruential type are discussed. They are known now to be essentially equivalent but are formulated incorrectly and the computational algorithms to implement the tests are unnecessarily complicated. New algorithms for these tests will be sketched.

TABLE OF CONTENTS

I. INTRODUCTION

The history of digital computing is characterized by the near exponential progress in hardware, operating systems, programming languages, and numerical computing algorithms. In contrast, the science of pseudo-random number generation has virtually stood still for the last twenty five years in spite of literally hundreds of publications on the subject.

D. H. Lehmer proposed the linear congruential scheme for the generation of pseudo-random numbers on a digital computer in 1951. This scheme has been the singularly most popular method ever since. Recently, feedback shift-register methods have been proposed for pseudo-random number generation but they have not achieved as widespread use.

It is essential to recognize the fact that neither method produces truly "random" numbers by any definition of randomness. Consequently, a great deal of effort has been invested in examining the sequences produced by random number generators to establish whether they meet statistical tests for randomness for relatively short samples. Given that a generator has "passed" an acceptable battery of statistical tests, its sequence is considered adequate for use in simulation experiments.

An elaborate collection of statistical tests has been developed over the years and Knuth [Ref. 8] provides an

excellent discussion of these tests. They are, however, not sufficient for certifying the quality of a generator. The report by Learmonth and Lewis [Ref. 9] attests to this fact in that for certain generators known through use to be poor, the statistical tests were not conclusive in identifying their weaknesses.

The recent work on testing Lehmer congruential random number generators has concentrated on characterizing the entire periodic sequence. The two tests proposed, which are essentially similar, are the lattice test and the spectral test. These tests provide deterministic rather than statistical criteria for rating the quality of the sequences.

The thesis to be examined here is that although these two tests are a significant advance in the testing of Lehmer congruential random number generators, they are formulated incorrectly and the computational algorithms to implement the tests are unnecessarily complicated.

It will be shown that the proper space in which to characterize finite periodic sequences is an algebraic group rather than the space of the natural numbers or the real line as has been previously assumed. The development to follow will concentrate on the class of primitive root/prime modulus random number generators which form a more general algebraic system, a finite field.

The special properties of finite field arithmetic will be developed and several new theorems will be presented

regarding primitive roots of prime fields. Using these properties of finite fields, the structure of linear congruential sequences on finite fields will be examined.

The conventional lattice and spectral tests will be defined and their algorithms outlined. These two tests will then be recast for finite field assumptions. New algorithms will be sketched as potential replacements for the lattice and spectral tests.

While the surface will only be scratched, the underlying theory presented will form the basis for future research in random number generator testing.

II. FINITE FIELDS

In this section, it is intended to make a critical reevaluation of the assumptions underlying the mathematical characterizations of linear congruential sequences. Both the spectral test of Coveyou and Macpherson and Knuth and the lattice test of Marsaglia and Ahrens and Dieter makes the very important assumption of an infinite sequence of integers. As will be shown, for the spectral test this assumption is critical for the development of the equidistribution properties of linear congruential sequences. Although the lattice test does not require this assumption, it is inherent in the development of the computational algorithm.

Abandoning this assumption and using the more appropriate assumption of a finite sequence, it will be seen that both the theoretical as well as computational development will be considerably more clear and concise.

A. FINITE FIELDS

The integers resulting from the linear congruential equation defining a random number generator from an algebraic group. A group is defined as a set of elements upon which is defined a binary operation called multiplication with the following properties:

1. the operation is closed, that is if a and b are elements of the group then c = ab is also in the group;

2. the operation is associative, that is

$$a(bc) = (ab)\ c \quad ;$$

3. there is an identity element in the group, usually denoted by the integer 1 such that $1a = a$ holds for every element a of the group;

4. for each element a of the group there is an inverse denoted a^{-1} such that $a^{-1}\ a = 1$.

The residues which are relatively prime to a general modulus m under the operation of multiplication modulo m form a group as defined above. When the group operation is multiplication, the group is called a multiplicative group. Similarly, an additive group may be defined with the group operation being addition. The inverses in the multiplicative group fill the role of division. For additive groups, the inverse is subtraction and the identity element is 0, i.e., $a + 0 = a$. In either case, if the group operation is also commutative, $ab = ba$ or $a + b = b + a$, the group is given another adjective, Abelian.

To recapitulate, for a random number generator $X_{i+1} \equiv a\ X_i \pmod{m}$ where m is composite, the integer residues form a finite Abelian multiplicative group under the operation of modulo multiplication. For the present case the residues of the random number generator $X_{i+1} \equiv a\ X_i \pmod{p}$, where p is prime, form a more general algebraic system,

specifically they form a finite field. A field is a generalization of a group wherein the group operations of addition, subtraction, multiplication, and division are all defined either as group operations or their respective inverses.

It is the arithmetic properties of finite fields that will reveal the structure of the linear congruential sequences.

B. FINITE FIELD ARITHMETIC

Given a finite field as the algebraic structure on which the residues from the random number generator are defined, it remains to examine how the ordinary arithmetic operations work in this system.

Modulo addition works as would be expected. In ordinary addition over the integers, the only solution to the equation $a + x = 0$ is $x = -a$. In finite field arithmetic over the positive integers the solution is given by another positive integer called the additive inverse. For example, in the finite field formed by the prime 17, the additive inverse of the integer 3 is not -3 but 14

$$3 + 14 = 17 \equiv 0 \pmod{17}$$

Therefore $x = 14$ satisfies $a + x = 0$ in this finite field.

Modulo multiplication also works as in conventional arithmetic. The multiplicative inverse, which plays the role of a divisor is somewhat differently defined. In ordinary arithmetic over the integers the solution to $ax = 1$ is

uniquely $x = 1/a = a^{-1}$. In finite field arithmetic, the role of a^{-1} is taken by another positive integer in the field. Again referring to the field formed by the prime 17, the solution to $3x = 1$ is $x = 6$, i.e., $3 \times 6 = 18 \equiv 1 \pmod{17}$. Therefore $3^{-1} = 6$ in this field.

Although subtraction and division are defined as the inverses of the field operations of addition and multiplication, the algebra of equations over the finite field becomes more difficult. The absence of negatives makes solutions to simple equations such as $3 - x = 7$ impossible.

Since the labelling of the field elements as positive integers was arbitrary, it is possible to relabel the elements more conveniently. One such relabelling, is as follows,

$$\{-\tfrac{1}{2}(p-1), -\tfrac{1}{2}(p-3), \ldots, -1, 0, 1, \ldots, \tfrac{1}{2}(p-3), \tfrac{1}{2}(p-1)\}$$

Here the elements previously labelled with integers greater than $\frac{1}{2}(p-1)$ are mapped into their additive inverses which are less than or equal to $\frac{1}{2}(p-1)$ and of opposite algebraic sign. For instance, in the field formed by the prime 17, the positive integer 14 is mapped into the element -3. This mapping preserves the additive inverse of 3 since $3 + (-3) = 0$ as required. This new notation will be called the primitive mark notation.

C. PRIMITIVE ROOTS

Before examining the structure of linear congruential sequences, it will be instructive to examine primitive roots of primes in the context of finite fields. As previously indicated, for the type of random number generators to be examined here, namely the primitive root/prime modulus type, the multiplier is required to be a primitive root to guarantee a full period. In finite field terminology primitive roots are termed generators of the field.

The term generator derives from the finite analogy of a generating function. Any primitive root of the prime finite field may be used in defining the generating function on the finite field. The term primitive root also has the very special connotation of primitive root of unity. A primitive root serves for a finite field the same special properties that the primitive root of unity $\exp\{2\pi ik\}$ serves for the complex field. In fact, the (infinite) field of complex numbers is the only other field which possesses a primitive root of unity.

While it is known that every prime possesses at least one primitive root, the only other significant fact that number theory offers is that each prime p contains precisely $\phi(p-1)$ primitive roots. Here $\phi(p-1)$ is Euler's totient function which is defined to be the number of integers less than and relatively prime to (p-1). When constructing a primitive root/prime modulus random number generator the greatest problem lies in discovering a primitive root of the

given prime. The procedure usually followed is to use a trial and error technique on small integers and then to apply the definition of a primitive root to verify if the number is in fact primitive. This actually is not an easy task since showing that p-1 is the least positive exponent such that $a^{p-1} \equiv 1 \pmod{p}$ requires considerable computation. Tables do exist listing several primitive roots for some primes and this is a great help. Knowledge of one primitive root provides a rather easy method for finding others. A simple, but potentially very lengthy algorithm for finding all the primitive roots of a given prime is as follows.

Algorithm A:

A1. Factor p-1 into its prime factors. (A sieve method may be used.)

A2. Select a known primitive root, say a; set k = 1.

A3. Divide k by each of the prime divisors of p-1. If any of the prime divisors divides k evenly, i.e., no remainder, then a^k is not a primitive root, go to A4. Otherwise print a^k as a primitive root.

A4. If k is greater than or equal to p-2, stop, all primitive roots have been found and printed; otherwise k = k+1, go to A3.

Viewing primitive roots as generators of the finite field of characteristic p, it is possible to use the properties of finite fields to discover further knowledge about other

primitive roots. All finite field elements may be represented as power residues of a primitive root of the field, that is, every element may be represented as $a^k \pmod p$ for a unique k. The multiplicative inverse of any finite field element is found easily using the following lemma.

Lemma 1: The multiplicative inverse of a finite field element (not necessarily a primitive root), $a^k \pmod p$, is simply $a^{(p-1)-k} \pmod p$.

Proof: $a^k a^{(p-1)-k} \equiv a^k a^{(p-1)} a^{-k} \pmod p$

$$\equiv 1 \pmod p$$

since $a^{(p-1)} \equiv 1 \pmod p$ by definition of a primitive root. Q.E.D.

This lemma leads to the following theorem concerning the multiplicative inverses of primitive roots.

Theorem 1: If a is a primitive root of the prime p, then its multiplicative inverse $a^{-1} \equiv a^{(p-2)} \pmod p$ is also a primitive root.

Proof: The multiplicative inverse of a is, by Lemma 1,

$$a^{-1} \equiv a^{(p-1)-1} \equiv a^{(p-2)} \pmod p.$$

To show that $a^{-1} \equiv a^{(p-2)} \pmod p$ is a primitive root of p, it must be shown that (p-1) is the least positive exponent such that

$$(a^{-1})^{(p-1)} \equiv (a^{(p-2)},^{(p-1)} \equiv 1 \pmod{p} .$$

Hence,

$$\begin{aligned}(a^{-1})^{(p-1)} \equiv (a^{(p-2)},^{(p-1)} &\equiv a^{(p-2)p}\ a^{-(p-2)} \\ &\equiv a^{(p-1)(p-1)-1}\ a^{-(p-2)} \\ &\equiv 1\ a^{-1}\ a^{-(p-2)} \\ &\equiv a^{(p-2)}\ a^{-(p-2)} \\ &\equiv 1 \pmod{p}.\end{aligned}$$

Assume $(a^{(p-2)},^{q} \equiv 1 \pmod{p}$ with $0 < q < (p-1)$, then

$$(a^{(p-2)},^{q} \equiv a^{(p-1)q}\ a^{-q} \equiv a^{-q} \pmod{p} .$$

Applying Lemma 1 again

$$a^{-q} \equiv a^{(p-1)-q} \pmod{p} .$$

If a^{-q} is congruent to 1 modulo p this would imply $a^{(p-1)-q}$ is also congruent to 1 and this contradicts the assumption that a is itself a primitive root, i.e., (p-1) is not the least positive exponent such that $a^{(p-1)} \equiv 1 \pmod{p}$. Q.E.D.

If the multiplicative inverse of a primitive root is also a primitive root then it would be logical to examine additive inverses. Unfortunately the case for additive inverses is somewhat more restrictive. To examine the additive inverses of primitive roots it is necessary to separate the primes into two classes, specifically the classes $p \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$ for primes $p > 2$. It is trivial to see that these are the only two classes into which the primes fall modulo 4.

Theorem 2: If a is a primitive root of the prime $p > 2$, then the additive inverse of a is also a primitive root of p if and only if $p \equiv 1 \pmod 4$.

Proof: In the unambiguous notation of primitive mark representation, the additive inverse of a primitive root a is -a. To show that -a is a primitive root of p when $p \equiv 1 \pmod 4$,

$$(-a)^{(p-1)(\mathrm{mod}\ 4)} \equiv (-a)^0 \equiv 1 \pmod p.$$

To show that -a is not a primitive root of p when $p \equiv 3 \pmod 4$,

$$(-a)^{(p-1)(\mathrm{mod}\ 4)} \equiv (-a)^2 \equiv a^2 \equiv 1 \pmod p.$$

Since it was assumed that a was a primitive root of p, the above contradicts the primitivity of a, i.e., p-1 is not the least positive integer such that $a^{(p-1)} \equiv 1 \pmod p$ for primes $p > 2$. Q.E.D.

The two theorems just presented offer some insight into the distribution of primitive roots over a prime finite field. Theorem 2 is particularly instructive when considering the field integers in their primitive mark representation. Knowing that the additive inverses are also primitive roots for certain primes, the $\phi(p-1)$ primitive roots are distributed symmetrically about the origin at 0. Considering again the finite field formed by the prime ($17 \equiv 1 \pmod 4$), there are $\phi(16) \equiv 8$ primitive roots distributed as follows:

-8 -7 -6 -5 -4 -3 -2 -1 0 1 2 3 4 5 6 7 8

The respective multiplicative inverses are indicated.

For the case of primes $p \equiv 3 \pmod 4$, the situation is less appealing. Since the additive inverses are not primitive roots, the symmetry is lost. There is no particular pattern to the distribution of the primitive roots or their multiplicative inverses.

III. STRUCTURE OF LINEAR CONGRUENTIAL SEQUENCES

The attempts to characterize the sequences emanating from linear congruential random number generators recently have focused on structural representations. The lattice test imposes a grid on the generated n-tuples of points and characterizes the sequences in terms of the lengths of the sides of the smallest n-dimensional hypercube which can be constructed. The spectral test, which can be shown to be a variant of the lattice test, views the n-tuples as forming waves of hyperplanes and characterizes the sequence bythe "frequency" of these waves.

Marsaglia [Ref. 9] attempted to expose more of the repetitive structure of the generated sequences. Three new theorems will be presented here to further characterize the structure of these sequences. By exploiting the primitive mark notation for finite fields more insight will be gained. These new theorems will then be contrasted with Marsaglia's work, leading to a redevelopment of the lattice test and spectral test.

A. THE FUNDAMENTAL SUBSEQUENCE

It is known that the period of a primitive root/prime modulus random number benerator is (p-1). Using the positive integer representation for the elements of the finite field, the sequence appears to have full period. The following theorem will establish the existence of a more fundamental half sequence.

Theorem 3: The sequence of (p-1) integers generated by a primitive root/prime modulus random number generator, when expressed as primitive marks, consists of a fundamental subsequence of length $\frac{1}{2}(p-1)$. This fundamental subsequence is followed by a replicate subsequence identical to the first except for opposite algebraic sign. These two subsequences, each of length $\frac{1}{2}(p-1)$ constitute the effective period of length (p-1).

Proof: Without loss of generality, let the sequence begin with $x_0 = 1$, then $x_1 = a$, the primitive root multiplier. In general, the k^{th} element is $x_k \equiv a^k \pmod{p}$. After generating $\frac{1}{2}(p-1)$ elements of this sequence, the next integer element is

$$x_{\frac{1}{2}(p-1)} \equiv 2^{\frac{1}{2}(p-1)} \pmod{p} .$$

Now, by definition of a primitive root, $a^{(p-1)} \equiv 1 \pmod{p}$, therefore

$$x^2_{\frac{1}{2}(p-1)} \equiv (a^{\frac{1}{2}(p-1)})^2 \equiv a^{(p-1)} \equiv 1 \pmod{p} .$$

This implies that $x_{\frac{1}{2}(p-1)} \equiv \pm 1 \pmod{p}$. In fact, $x_{\frac{1}{2}(p-1)} \equiv -1 \pmod{p}$ (the primitive mark representation of $(p-1)$). Since it is known that each integer appears once and only once in the sequence and +1 appeared as x_0, therefore, beginning with element $x_{\frac{1}{2}(p-1)}$, the same fundamental subsequence of primitive marks repeats with opposite algebraic sign. Q.E.D.

For illustration, consider the following example using the prime modulus 17 and primitive root 3.

Deviate	X_0	X_1	X_2	X_3	X_4	X_5	X_6	X_7	X_8	X_9	X_{10}	X_{11}	X_{12}	X_{13}	X_{14}	X_{15}	X_{16}
Positive integer	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1
Primitive mark	1	3	-8	-7	-4	5	-2	-6	-1	-3	8	7	4	-5	2	6	1

FIGURE 3.1 $X_{i+1} \equiv a\, X_i \pmod{p}$; $a = 3$, $p = 17$

For the lattice test, the consequences of this theorem are not particularly important. The grid formed by the lattice of n-tuples is very easily constructed using very few n-tuples and its regularity is apparent without having to generate the entire sequence. For the spectral test, however, the ffect would be a folding of the sequence onto itself.

The next theorem relates the properties of multiplicative inverses to the resulting sequence generated by primitive root/prime modulus random number generators.

Theorem 4: In the primitive root/prime modulus random number generator $X_{i+1} \equiv a\, X_i \pmod{p}$, replacing the multiplier a by its multiplicative inverse, a^{-1}, results in a generated sequence which is precisely the reverse of the sequence generated by a.

Proof: The sequence produced by $X_{i+1} \equiv a\, X_i \pmod{p}$ starting with $X_0 = 1$ is $X := \{1, a, a^2, \ldots, a^{(p-2)}, a^{(p-1)}\} \pmod{p}$. The sequence produced using the inverse a^{-1} starting with $X_0^* = 1$ is $X_0^* := \{1, (a^{-1}), (a^{-1})^2, \ldots, (a^{-1})^{(p-2)}, (a^{-1})^{(p-1)}\} \pmod{p}$. By definition of a primitive root, $a^{(p-1)} \equiv 1 \pmod{p}$ therefore,

$$1 \equiv X_0^* \equiv X_{(p-1)} \equiv a^{(p-1)} \equiv 1 \pmod{p}.$$

Similarly,

$$a^{-1} = X_1^* = X_{(p-2)} = a^{(p-2)} \equiv a^{(p-1)}a^{-1} \equiv a^{-1} \pmod{p}.$$

By induction, for the general element X_k^*, the corresponding element of X is $X_{(p-k-1)}$, (see Lemma 1),

$$a^{-k} = X_k^* = X_{(p-k-1)} = a^{(p-k-1)} \equiv a^{(p-1)}a^{-k} \equiv a^{-k} \pmod{p}.$$

Q.E.D.

Clearly, the sequence generated when the multiplicative inverse is substituted, is precisely the reverse of the one generated using the original primitive root. Application of Theorem 3 will reveal that the fundamental subsequences are reversed also.

Essentially, substituting the multiplicative inverse for the primitive root multiplier causes the random number generator to run "backwards."

For the special case of prime moduli such that $p \equiv 1 \pmod 4$, substituting the additive inverse for the primitive r-ot multiplier results in further interesting properties of the sequence as the following theorem demonstrates.

Theorem 5: In the primitive root/prime modulus generator $X_{i+1} \equiv a\, X_i \pmod p$, where $p \equiv 1 \pmod 4$, replacing a by its additive inverse, -a, results in a generated sequence with every odd numbered element of the sequence replaced by its additive inverse. Expressed in primitive mark notation, the fundamental subsequences are the same as for the multiplier a except that the odd numbered elements have opposite algebraic sign.

Proof: Without loss of generality, let the sequence $X_{i+1} \equiv a\, X_i \pmod p$ begin with $X_0 = 1$, then the generated sequence is

$$X: = \{1,\ a,\ a^2,\ \ldots,\ a^{(p-2)},\ a^{(p-1)}\} \pmod p \quad .$$

It was shown in the proof of Theorem 3 that $a^{\frac{1}{2}(p-1)} \equiv -1 \pmod p$, hence $a^{\frac{1}{2}(p-1)+1} \equiv a^{\frac{1}{2}(p-1)}\ a \equiv -1\, a \equiv -2 \pmod p$. That is, $a^{\frac{1}{2}(p-1)+1}$ is the additive inverse of a. The sequence generated by $X^*_{i+1} \equiv (-a)\, X^*_i \pmod p$ beginning with $X^*_0 = 1$ is

$$X^*: = \{1,\ (-a),\ (-a)^2,\ \ldots,\ (-a)^{(p-2)},\ (-a)^{(p-1)}\} \pmod p .$$

The elements $(-a)^k$ for k even is X* are obviously equal to the elements a^k in X. The elements $(-a)^k$ for k odd, that is, the odd numbered elements of X* are the additive inverses of the elements a^k in X in primitive mark notation,

$$a^k + (-a)^k \equiv a^k - a^k \equiv 0 \pmod{p} .$$

The second part of the theorem follows directly from Theorem 3. Q.E.D.

Where Theorem 4 showed how to reverse the sequence using the multiplicative inverse, using the additive inverse effects a "half shuffle" of the sequence.

B. MARSAGLIA'S THEOREMS

Marsaglia [Ref. 9] disucssed the idea of a "fundamental sequence" for the third generator $X_{i+1} \equiv a X_i + b \pmod{m}$ where m is composite. This theorem will be presented here and then contrasted with Theorem 3.

Theorem 6 (Marsaglia [Ref. 9]): The choice of b and the starting value X_0 are of no consequence for the generator $X_{i+1} \equiv a X_i + b \pmod{m}$, in the sense that if X_0, X_1, X_2, ... is any sequence generated by $X_{i+1} \equiv a X_i + b \pmod{m}$ and if Y_0, Y_1, Y_2, ... is the fundamental sequence 0, 1, 1+a, $1+a+a^2$, ..., generated by $Y_{i+1} \equiv a Y_i + 1 \pmod{m}$, then there are constants V and W such that $X_i = V Y_i + W$. In

fact, $V = X_0(a-1) + b$ and $W = X_0$. Thus the sequence of the form $X_{i+1} \equiv a\ X_i + b \pmod{m}$ with X_0 and b arbitrary (including $b = 0$) may be obtained from an affine transformation of the fundamental sequence.

In addition, if the multiplier a is relatively prime to m, then the period of the sequence $X_0, X_1, X_2, \ldots$ with $X_{i+1} \equiv a\ X_i + b \pmod{m}$ is the period of the fundamental sequence for modulus m/d where $d = \gcd\{m, X_0(a-1) + b\}$. (End of theorem).

For the case of the primitive root/prime modulus generator, $m = p$, a prime, a is a primitive root of p, and $b = 0$. With no loss of generality, for $X_0 = 1$

$$d = \gcd\{p, (a-1)\} = 1$$

since $(a-1)$ and all other integers less than or equal to $(p-1)$ are relatively prime to p. Therefore the period of this fundamental sequence is theperiod of the sequence for $p/d = 1$ or $(p-1)$ as is already known. The sequence generated by $X_{i+1} \equiv a\ X_i \pmod{p}$ can be put simply into one-to-one correspondence with the sequence {4} in the theorem. In the case of the primitive root/prime modulus generator, Marsaglia's theorem is completely uninstructive, and by using positive integer notation, it actually misses the existence of the fundamental subsequences of Theorem 3 which uses primitive mark notation.

Marsaglia provides another theorem which attempts to uncover more detail about his fundamental subsequences. It is presented here.

Theorem 7 (Marsaglia [Ref. 9]): Let a be relatively prime to the modulus m and have multiplicative order[1] t. Then the fundamental sequence:

$$Y_0 = 0,\ Y_1 = 1,\ Y_2 = 1+a,\ Y_3 = 1+a+a^2,\ \ldots$$

$$Y_{i+1} \equiv 1 + a\,Y_i \pmod{m} \qquad (1)$$

is made up of a block $\{B\} = \{Y_0, Y_1, \ldots, Y_{t-1}\}$ of t distinct residues of m, followed by translates of that block $\{B\}$, $\{B+c\}$, $\{B+2c\}$, ... where $c = 1+a+a^2+ \ldots +a^{(t-1)} \pmod{m}$. The period of the sequence (1) is tr, where r is the additive order of c: $r = m/\gcd\{c,m\}$.

Applying this theorem to the primitive root/prime modulus case where m = p, a prime, b = 0, and a is a primitive root of p, it is clear that t = (p-1) by definition of a primitive root. Therefore, Marsaglia's fundamental sequence is made up of a block $\{B\} = \{Y_0, Y_1, \ldots, Y_{(p-2)}\}$ of the (p-1) distinct residues of p,i.e., the sequence constitutes one block of length (p-1). For the additive order of c,

---

[1]Multiplicative order is defined as the least positive integer t such that $a^t = 1 \pmod{m}$ when $\gcd\{m,a\} = 1$.

$$c = 1 + a + a^2 + \ldots + a^{(p-2)} \pmod{p} = \sum_{j=0}^{p-2} a^j \pmod{p}$$

$$= \frac{1 - a^{(p-1)}}{1 - a} \pmod{p}$$

$$= 0;$$

$$r = p/\gcd\{0,p\} = p/p = 1 \quad \text{and} \quad tr = (p-1).$$

As in the case of Theorem 6, this theorem provides no information. Theorem 3 offers much more insight into the structure of the linear congruential sequence. The recognition of the finite field and using primitive mark notation provide the basis for the redevelopment of the lattice test and spectral test.

IV. THE LATTICE TEST

The use of the lattice test is a fairly recent development even though its proposal as a means of characterizing linear congruential sequences goes back at least twelve years. Franklin [Ref. 6] first observed the hyperplane structure of n-tuples from a linear deterministic sequence. He was concerned, however, with infinite sequences. Jansson's book [Ref. 7] reiterated the usefulness of the lattice and alluded to its possible use with finite, periodic sequences. He did not provide an algorithm or any computational results.

Marsaglia's famous paper [Ref. 10] focused widespread attention on the hyperplane structure of the sequences produced by congruential generators. Papers by Beyer, Roof, and Williamson [Ref. 4] and Smith [Ref. 13] published the first algorithms and computational results.

Recent results on the lattice structure of popular generators come chiefly from the later paper of Marsaglia [Ref. 9] and the as yet unpublished book by Ahrens and Dieter [Ref. 2]. Both of these references contain computational algorithms for performing the test. It is the difficulty of implementing these algorithms on a digital computer which inspired the work to follow.

A. THE ALGORITHMS

The current algorithmic implementations of the lattice test will now be described with emphasis on the assumptions made. Marsaglia's algorithm, BEST2, will be discussed first.

In n-dimensional space, it is assumed that a set of points $b_1, b_2, \ldots, b_n$ exist such that all points in the space are integral multiples of them, that is,

$$\{r_1b_1 + r_2b_2 + \ldots + r_nb_n;\ r_1,r_2, \ldots, r_n = 0,\pm1,\pm2, \ldots\}$$

constitutes the set of all points spanned by $b_1, b_2, \ldots, b_n$. These points then form a lattice in n-space.

The points $b_1, b_2, \ldots, b_n$ are actually n-vectors so that when viewed as rows of a matrix they form a basis for the points in n-space. Any set of n linearly independent vectors forms a basis for the points generated by the linear congruential generator. The objective of the lattice test is to start with an initial basis and reduce it through elementary row operations to a so-called optimal basis. The characterization of the sequence is given by the ratio of the longest side to the shortest side of the optimal hypercube defined by the reduced basis vectors.

Ideally, all of the points in n-space will be generated so that the optimal lattice basis will have all sides of length one and a unit cell volume of one. Since a linear congruential generator produces only p points in n-space where p is the modulus of the generator, the unit cell volume

will be p^{n-1}. For a good generator, the ratio of longest to shortest side will be close to one, indicating a semblance of regularity of distribution of the points. An ad hoc rule is to summarily reject any generator whose side ratio is greater than two.

A natural starting basis for the case of n = 2 is given by the vectors

$$(1,a) \qquad \text{and} \qquad (0,p)$$

where p is the modulus of the generator. These basis vectors are derived as follows:

$$X_{i+1} = a\, x_i - kp$$

$$X_{j+1} = a\, x_j - lp$$

for some integers k and l, so

$$(x_j, x_{j+1}) - (x_i, x_{i+1}) = (L, aL-(l-k)p)$$

where L is the integral distance between X_j and X_i. In basis vector form $(X_j, X_{j+1}) - (X_i, X_{i+1}) = L(1,a) - (l-k)(0,p)$ hence the vector difference between any two generated points is the sum of integral multiples of the two basis vectors (1,a) and (0,p). This form of a starting basis can naturally be generalized to an n-dimensional basis.

Marsaglia formalizes this basis concept with a theorem for the lattice in 3-space.

Theorem 8 (Marsaglia [Ref. 9]): Let $a_1, a_2, \ldots, a_m$ be the set of points in 3-space of the form (x_i, x_{i+1}, x_{i+2}) where the X's are reduced residues of some modulus m generated by the congruential generator $X_{i+1} \equiv a\, x_i + c \pmod{m}$. There is no restriction on the integers c, a, or m. If the point b = (0, c, ac+c) is subtracted from each of these points, then the resulting points, $a_1-b, a_2-b, \ldots, a_m-b$ all lie on a lattice with unit cell volume m^2, generated by the 3 points $(1, a, a^2)$, (0, m, 0) and (0, 0, m).

The generalization to higher dimensions is straightforward; for example, in 4-space, if $b = (0, c, ac+c, a^2C+ac+c)$ is subtracted from each of the points of the form $(x_i, x_{i+1}, x_{i+2}, x_{i+3})$, then the resulting $a_1-b, a_2-b, \ldots, a_m-b$ all lie on a lattice with unit cell colume m^3 generated by the 4 points $(1, a, a^2, a^3)$, (0, m, 0, 0), (0, 0, m, 0) and (0, 0, 0, m).

For comparative purposes, this initial basis is of no use. The object of the lattice test is to employ elementary row operations on the rows of the initial basis, or unimodular transformations to the basis matrix, to acquire an optimal, or nearly optimal, basis which can be used to compare generators.

To this end, Marsaglia [Ref. 9] offers the following algorithm.

Algorithm BEST 2

Given two points $a = (a_1, a_2, \ldots, a_n)$ and $b = (b_1, b_2, \ldots, b_n)$ in n-space

B1. If b is shorter than a, interchange b and a.

B2. Replace b by b - La, where L is the integer closest to

$$ab'/aa' = \Sigma a_i b_i / \Sigma a_i^2.$$

B3. If the new b is longer than a, stop. Otherwise, go to step B1.

BEST2 starts with the initial basis vectors defined above. Upon termination, the first row contains the shortest reduced basis vector and the last row contains the longest reduced basis vector. The ratio of these two basis vectors characterizes the lattice produced by the generator in question.

To further understand the implementation of the lattice test using BEST2, Marsaglia [Ref. 9] gives the following example for the case of n = 4.

Algorithm N

N1. Start with a basis a_1, a_2, a_3, a_4 ordered in terms of increasing (Euclidean) length $|a_1| \leq |a_2| \leq |a_3| \leq |a_4|$. For the congruential generator $T(X) = ax + b \pmod m$, a basis is $(1, a, a^2, a^3)$, $(0, m, 0, 0)$, $(0, 0, m, 0)$, $(0, 0, 0, m)$.

N2. Apply the BEST2 algorithm to a_1, a_2 then to a_1, a_3 then to a_1, a_4 then to a_2, a_3 then to a_2, a_4 then to a_3, a_4. If these 6 applications of BEST2 do not change any of a_1, a_2, a_3, a_4 then stop. Otherwise order the new basis and repeat this step until the 6 applications of BEST2 produce no change.

N3. If $|b_1| \leq |b_2| \leq |b_3| \leq |b_4|$ is the basis on which 6 applications of BEST2 have no effect, use the ratio $r = |b_4|/|b_1|$ to characterize the lattice. A ratio r near 1 means a good lattice and a large r means a bad lattice. Typically, good lattices have $r < 2$ while $r > 3$ might be defined as a bad lattice.

The implementation just presented has become popular for implementation on digital computers. Later in this section, the inherent computational problems of this algorithm will be pointed out.

In Marsaglia's own terminology the repeated application of the BEST2 algorithm results in a nearly optimal basis. In certain cases it arrives at the optimal, or fully reduced basis. In certain cases it arrives at the optimal, or fully reduced basis. Preceeding the work of Marsaglia, Beyer, Roof, and Williamson [Ref. 4] formulated an algorithm for obtaining the optimal, fully reduced basis. They approached the problem of obtaining the basis which would yield shortest vector lengths as a problem in the solution of positive definite quadratic forms. In his work on the theory of the

geometry of numbers, the famour German mathematician Minkowski established criteria for fully reduced basis vectors. Ahrens and Dieter [Ref. 2] also use the Minkowski theory in developing their algorithm which will now be presented.

A great deal of preliminary definitions and lemmas are necessary to adequately establish reduced bases in the Minkowski sense. They will not be repeated here but the algorithms themselves will be presented to indicate the computations necessary for achieving reduced bases.

Ahrens and Dieter propose two algorithms, one for the case of two dimensions and one for the cases $2 < n \leq 6$. It should also be noted that full reduction of the basis vectors in the Minkowski sense has only been proven for $n \leq 4$. For the cases $n = 5$ and $n = 6$ the sufficiency of Minkowski's criteria has not been proven and for the cases $n > 6$ no criteria exist.

For the two dimensional case the following algorithm produces a Minkowski reduced basis for the lattice of a linear congruential sequence.

Algorithm MB2.

M1. Set $i = 1$, $j = 2$, and $s = 0$.

M2. Set $m = [\frac{1}{2} + (b_i b_j)/(b_i b_i)]$.

M3. If $m \neq 0$, go to M5.

M4. Set $s = s+1$. If $s = 2$, go to M7, otherwise go to M6.

M5. Set $b_j = b_j - mb_i$ and $s = 0$.

M6. Interchange the values of i and j. Go to M2.

M7. If $|b_1| > |b_2|$, interchange b_1 and b_2.

M8. Return the Minkowski basis b_1, b_2.

It is assumed that b_1 and b_2 are an initial basis as in the Marsaglia algorithm. In step M2, the bracket notation represents a truncation to the next smallest integer value. Products such as $(b_i b_j)$ represent ordinary vector dot products.

Full reduction in the cases n = 3 to n = 6 requires an auxiliary table, C_n, of 5560 coefficients. These may be precomputed and stored or they may be computed within the algorithm as they are required. The algorithm for these cases is as follows.

Algorithm BMi.

BM1. Sort the b_i such that $|b_1| \leq |b_2| \leq |b_3| \leq \cdots \leq |b_n|$.

BM2. Search for an expression

$$m = [\tfrac{1}{2} + (b_i b_j)/(b_i b_i)]$$

which is not zero. If no such n exists, set k = 4 and go to BM4.

BM3. Set $b_j = b_j - m\, b_i$, restore the order and go to BM2.

BM4. Set j = n and $v = \sum_{i=1}^{n} c_i b_i$ where the c_i constitute the k-th set of coefficients in the table C_n.

BM5. If $c_j = 0$ or if the greatest common divisor $d = (c_j, \ldots, c_n)$ is not 1 set j = j-1 and restart this step. (The test of d is easy since $d \neq 1$ occurs in only four possible cases.) If $vv < b_j b_j$, go to BM7.

BM6. If k points at the last vector in the table C_n (i.e., if k = 26, 80, 402, 4952 for n = 3, 4, 5, 6) go to BM8. Otherwise set k = k+1 and go to BM4.

BM7. Set b_j = v restore the order $|b_1| \leq |b_2| \leq \ldots \leq |b_n|$ and go to BM2.

BM8. Return the Minkowski basis $b_1, b_2, \ldots, b_n$.

The table, C_n, is used to insure that there remain no unimodular transformations which will further reduce a given pair of basis vectors. In many cases the basis vectors cannot be further reduced. Here the Marsaglia algorithm and the Ahrens and Dieter algorithm would stop at identical bases. The Ahrens and Dieter algorithm proceeds, however, when further reduction is possible. Ahrens and Dieter offer no theory indicating which multipliers require the additional Minkowski reduction.

B. COMPUTATIONAL IMPLICATIONS

Both algorithms just presented are not so complicated that a programmer would have difficulty coding them for execution on a digital computer. Ahrens and Dieter provide a fairly straight forward method for constructing the table of coefficients, C_n. Marsaglia has provided examples of his own algorithm worked out, ostensibly by hand, for some two dimensional cases.

The real problems arise when it is realized that except for very small moduli, existing digital computers cannot express the values which arise during the course of the algorithm's execution.

In detailing the algorithms, no mention was made of reducing the integer values by the modulus. In fact, in the initial basis the modulus appears as the only non-zero element in n-1 of the basis vectors. The first vector similarly contains successively higher powers of the multiplier which can be assumed to eventually exceed the modulus in magnitude.

The modulus for a random number generator is typically chosen to be a value very close to the word size of the host computer. In attempting to implement the lattice test, a programmer is immediately confronted with the problem of expressing the values which exceed the modulus and consequently exceed the computer's word size. Knuth [Ref. 8] has advised that at least 90-bit integer arithmetic is required to accurately compute the desired results for moduli of the order 2^{35}. Needless to say, this requirement exceeds the capacity of existing general purpose computers. One known method to alleviate the problem is to acquire a software package which handles unlimited precision computations.

The computational problems are certainly a hinderance, but not insurmountable. It will now be shown that all of these problems are a result of the inappropriate formulation of the lattice test. By avoiding the over-sophistication of the previous development, useful results can be obtained fairly simply.

C. THE LATTICE TEST IN A FINITE FIELD

In Chapter II it was shown that by viewing the generated points as elements of a finite field, interesting properties of the structure of linear congruential sequences could be revealed. The use of the finite field construct was not a gimmick to achieve the results of that chapter. It is the only rational construct to use in examining these finite, periodic sequences.

All of the computational difficulties with the lattice test as described above arise from the decision of the authors to treat linear congruential sequences as infinite sequences of integers, or worse yet, as the field of real numbers. The modulus m (composite) or p (prime) is not an element of the field and cannot legitimately be expressed in the field. Likewise, the intermediate computations which result in values greater than the modulus represent quantities not in the field which is to be characterized.

The same concepts of finite field arithmetic which were applied to the individual elements of the field in Chapter II are readily extensible to the finite field of vectors in a finite n-dimensional space. Arithmetic in a finite vector space over a field will be examined and an intuitive development of the lattice test will now be presented.

Conceptually, an n-dimensional space defined on a finite field with p elements contains p^n distinct points or p^n vectors emanating from the origin (taken to be the vector additive

identity (0,0, ..., 0)). Arithmetic defined on these vectors possesses the field properties relating to the operations of addition and multiplication, that is the properties of closure, distributivity, commutativity, and the additive and multiplicative identities.

A linear congruential random number generator with primitive root multiplier and prime modulus produces a periodic sequence of (p-1) integers. Although the element zero does not appear explicitly, it will be agreed to include it to satisfy the requirement of an additive identity for field arithmetic. Hence the p elements (0,1,2, ..., p-1) are produced in some permuted order.

The multidimensional properties of a linear congruential sequence are derived from considering consecutive n-tuples of the generated elements. Although the n-dimensional finite vector space defined on a field of p elements contains p^n vectors, the set of n-tuples derived from a linear congruential sequence contains only p of these vectors, that is, the vectors

$$(\{X_0,X_1,\ldots,X_{n-1}\}, \{X_1,X_2,\ldots,X_n\}, \ldots, \{X_{p-1},X_0,\ldots,X_{n-2}\})$$

These p vectors satisfy the additive field property, that is, the sum of any two vectors is also a vector in the field. The additive identity is defined since for any vector, there is another vector such that their sum is $(p,p,\ldots,p) \equiv (0,0,\ldots,0) \pmod{p}$.

The lattice test need only be concerned with the p vectors generated by the linear congruential sequence regardless of the dimension of the space being considered. The optimal hypercube in n-dimensional space will be defined by n vectors of the p possible vectors. The lengths of sides of the hypercube will be the difference of the vectors defining adjacent corners of the hypercube, and by the properties of finite field arithmetic, this vector difference will also be one of the p possible vectors.

The previous development of the lattice test required a basis of n linearly independent vectors to span the space. This is a requirement only when all p^n vectors are to be spanned. Since only p^1 possible vectors are to be spanned in this formulation, only one basic vector is necessary. A natural starting basic vector is then $(1,a,\ldots,a^{n-1}) \pmod p$. It is clear that this vector is one of the p possible vectors and all other vectors are integral multiples of this basic vector. Reduction modulo p is carried out since the field operations are defined to be modulo addition and modulo multiplication. Problems of overflow are avoided since the vector elements never exceed p in magnitude.

The question of a new lattice test algorithm remains. Which integral multiples of the basic vector constitute the sides of the smallest n-dimensional hypercube formed by the p possible vectors?

The two dinensional case will be considered. In the finite two dimensional space over the prime field of

characteristic p, there are p^2 possible vectors. Given a primitive root/prime modulus random number generator $X_{i+1} \equiv a\ X_i \pmod{p}$, the full period will consist of a permutation of the (p-1) field elements. Again, it will be agreed to include the additive identity element 0. Taking successive, overlapping pairs of the elements of the linear congruential sequence results in p possible vectors in the finite space of p^2 vectors. Since the integer 1 appears in the sequence, the basic vector will be chosen to be (1,a). The order in which the vectors are generated is immaterial. By systematically choosing the vectors, the lattice spanned by the p vectors can be constructed without lengthy search.

Assuming the primitive root multiplier to be less than $\frac{1}{2}p$, the next vector of interest is the vector (2,2a) = 2(1,a). Clearly, this vector is one of the p possible vectors and it can also be seen that it is oriented in the same direction as (1,a) but with twice the magnitude. Another way to view this situation is to treat (1,a) and 2(1,a) as points which lie on the same line emanating from the origin (0,0), each point maintaining a constant distance from the preceeding point.

To determine how many points lie on this line it is necessary to determine which value k_1 causes the quantity $k_1 a$ to exceed the modulus p and consequently be reduced (mod p). With $k_1 a$ reduced (mod p), the vector $k_1(1,a) \pmod{p}$ is no longer oriented in the same direction as the vectors (1,a), 2(1,a), ..., $(k_1-1)(1,a)$. The value k_1 is simply

$[p/a]$ where the brackets indicate the greatest integer function.

Beginning with the point $k_1(1,a) \pmod p$ another line is formed parallel to the first line consisting of the points

$$\{k_1(1,a),\ (k_1+1)(1,a),\ \ldots,\ (k_2-1)(1,a)\} \pmod p.$$

The value k_2 is $[2p/a]$. This procedure may be continued for successive parallel lines until all p points have been covered.

It is, of course, not necessary to generate all of the p points nor is it necessary to determine how many parallel lines are contained in the space. To find the shortest vector emanating from the origin to one of the parallel lines requires at most a computation of the first element of the line. This bound is actually much greater than the number of computations required in practical situations. Assuming that the vector to a point $k_i(1,a) \pmod p$ has been computed, all starting points $k_j(1,a) \pmod p$ which lie on the same line need not be considered since they are parallel to the vector and obviously are greater in magnitude.

Some examples will now be shown to clarify the procedure described above.

Example 1. $X_{i+1} \equiv a\, X_i \pmod p$; $a = 3$, $p = 17$.
The basic vector is $(1,3)$. $k_1 = [17/3] = 6$, $k_2 = [34/3] = 12 > 3$. Only two vectors need be considered. The Euclidean

length of the vector (1,3) is $(10)^{1/2}$. The length of the vector (6,1) is $(37)^{1/2}$. To complete the search for the parallelogram with shortest sides, the vector (6,1) - (1,3) = (5,2) is computed and its length is $(29)^{1/2}$. The side ratio of the optimal lattice parallelogram is $(29)^{1/2}/(10)^{1/2}$ = 1.70.

Example 2. $X_{i+1} \equiv a\ X_i \pmod{p}$; a = 7, p = 17. The basic vector is (1,7). k_1 = 17/7 = 3, k_2 = 34/7 = 5, k_3 = 51/7 = 8 > 7. The respective lengths are $(50)^{1/2}$, $(25)^{1/2}$, and $(26)^{1/2}$. The vector (3,4) with the smallest length $(25)^{1/2}$ will be one side of the optimum lattice parallelogram. The distance from (3,4) to (5,1), the next smallest, will be computed to determine if it will yield a smaller side. Since this length is $(13)^{1/2}$, the optimum lattice parallelogram has side ratio $(25)^{1/2}/(13)^{1/2}$ = 1.39.

Example 3. $X_{i+1} \equiv a\ X_i \pmod{p}$; $a = 7^5 = 16{,}807$; $p = 2^{31} - 1$. The basic vector is (1,16807). $k_1 = 2^{31} - 1/16807 = 127774 > 16807$. The respective lengths are $(282475250)^{1/2}$ and $(16521383917)^{1/2}$. The length of the vector (127774,13971) to (1,16807) is $(16333982425)^{1/2}$. The side ratio of the two shortest sides is then $(16333982425)^{1/2}/(282475250)^{1/2}$ = 4.74.

Two interesting results should be noted here. First, this generator has less than optimal two dimensional lattice characteristics and second, the previously reported results for this generator used the ratio

$(16521383917)^{1/2}/(282475250)^{1/2} = 7.60$ from Marsaglia's algorithm. This is evidence of the Marsaglia algorithm BEST2 not achieving an optimal basis.

This chapter has unfortunately stopped tantalizingly short of producing an algorithm for use in the many cases of interest. The last chapter will outline the course of future work in this direction.

V. THE SPECTRAL TEST

The spectral test for linear congruential random number generators is directly related to the lattice test. The development of the spectral test comes from an entirely different theoretical basis, however.

The application of the spectral test to linear congruential random number generators began with the work of Coveyou and Macpherson. Knuth [Ref. 8] published a computational algorithm which, as stated in the previous chapter, requires 90-bit integer arithmetic to achieve accurate results. A brief historical outline of the basis and development of the spectral test will be given. The test will then be compared and contrasted with the lattice test.

A. HISTORICAL DEVELOPMENT

The theoretical basis of the spectral test for linear congruential sequences is a theorem by H. Weyl in 1916. The theorem was concerned with the distribution of sequences of deterministic numbers reduced modulo 1. Although the sequences to be examined were deterministic in nature, they were also assumed to be infinite in length and of infinite precision in representation.

Assuming an infinite sequence of real numbers, say $X_0, X_1, \ldots, X_n, \ldots$, on the half-open interval [0,1), select a number Y also on the interval [0,1). Let N_y be the cardinal number of the first N values of {X} which are contained in the

subinterval [0,Y). The sequence {X} is then said to be equidistributed modulo 1 if $\lim_{N\to\infty} N_y/N = Y$ for all values of Y. Weyl's theorem extends this definition to an arbitrary number of dimensions.

A 1963 paper by Franklin [Ref. 6] applied Weyl's theorem to sequences of pseudo-random numbers. Franklin was concerned with the equidistribution of the deterministic sequence $X_i = \theta^i \pmod 1$ for i = 1,2,.... He proved that this sequence is completely equidistributed for almost all $\theta > 1$ and further proved that θ must be a transcendental number. Franklin's work was also developed on the basis of infinite precision of the values $X_i \pmod 1$.

Although they do not cite Franklin's work as a precedent, Ahrens and Dieter [Ref. 3] have proposed a FORTRAN implementation of a random number generator using real arithmetic and the golden section number as a multiplier. This number is, of course, irrational but not transcendental. They claim the equidistribution properties of this generator are derived from the irrationality of the multiplier.

The Coveyou and Macpherson development was the first time that Weyl's theorem was applied to finite, periodic sequences of linear congruential generators. Knuth amplified the development of the Coveyou and Macpherson test and offered a complete algorithm for its implementation.

B. THE ALGORITHM

Weyl's theorem provides necessary and sufficient conditions for equidistribution of infinite sequences of deterministic numbers reduced modulo 1. To introduce Weyl's theorem, let $\overline{X}_i$, $i = 1,2,\ldots$ be a sequence of n-tuples, that is, $\overline{X}_i = (X_{0,i}, X_{1,i}, \ldots, X_{n-1,i})$ where the $X_{j,i}$ all lie in the interval $[0,1)$. The $\overline{X}_i$ are n-dimensional vectors in the n-dimensional unit hypercube in Euclidean space.

Weyl's Theorem.[1] The sequence of points $\overline{X}_1, \overline{X}_2, \ldots$ is equidistributed modulo 1 if and only if

$$\lim_{p\to\infty} \frac{1}{p} \sum_{j=1}^{p} \exp(-2\pi i(q_0 X_{0,j} + q_1 X_{1,j} + \ldots + q_{n-1} X_{n-1,j})) = 0$$

for all vectors $(q_0, q_1, \ldots, q_{n-1})$ with integer elements not all zero.

The proof of this theorem is rather lengthy and will not be repeated here. Coveyou and Macpherson [Ref. 5] applied this theorem to the case of linear congruential random number generators and provided computational details for an algorithm. Knuth's development [Ref. 8] of the algorithm will be outlined.

To begin, the spectral test is only applicable to full period generators, that is, properly formulated mixed

---

[1] Jansson, Birger, Random Number Generators, p. 156, Amlquist and Wiksell, Stockholm, 1966.

congruential generators with composite modulus or primitive root/prime modulus generators. Although Knuth treated the mixed congruential case, the primitive root/prime modulus case will be substituted in this brief outline.

Let the random number generator be $X_{i+1} \equiv a\ X_i \pmod{p}$. The finite Fourier transform of this sequence is then

$$f(s_1,s_2,\ldots,s_n) = \frac{1}{p} \sum_{k=0}^{p-1} \exp\left(\frac{-2\pi i}{p} (s_1X_k+s_2X_{k+1}+\ldots+s_nX_{k+n-1})\right)$$

$$= \frac{1}{p} \sum_{k=0}^{p-1} \exp\left(\frac{-2\pi i}{p} (s(a)X_k)\right)$$

where

$$s(a) = s_1 + s_2a + \ldots, s_na^{n-1}.$$

Since all values of k appear in the sequence and their order is immaterial, the following may be substituted:

$$f(s_1,s_2,\ldots,s_n) = \frac{1}{p} \sum_{k=0}^{p-1} \exp\left(\frac{-2\pi i}{p} s(a)k\right).$$

Noting that this represents the sum of a geometric series, the basis formula is

$$f(s_1,s_2,\ldots,s_n) = \delta(s(a)/p) \qquad (1)$$

where $\delta(X) = 1$ if X is integer and 0 otherwise.

Application of discrete probability theory yields the result that the joint probability of any n-tuple (X_k, X_{k+1}, ..., X_{k+n-1}) is $1/p^n$ hence the value $f(s_1,s_2,...,s_n)/p^n$ may be interpreted physically as the amplitude of the n-dimensional complex plane wave

$$\omega(t_1,t_2,...,t_n) = \exp(\frac{2\pi i}{p}(s_1t_1+...+s_nt_n)).$$

A wave number may assigned to this plane wave corresponding to the frequency of the wave. The wave number is

$$v = (s_1^2+s_2^2+...+s_n^2)^{1/2} \quad \text{for} \quad s_k \quad p/2.$$

In a truly random sequence no waves should be present except a constant wave of frequence zero. Any generator which produces a swquence whose transform yields nonzero frequencies can be considered to be nonrandom. To summarize the spectral test Knuth[2] states:

> "If v_n is the smallest nonzero value of the wave number ... for which $f(s_1,s_2,...,s_n) \neq 0$ in a linear congruential sequence with maximum period, then the sequence $X_0/m, x_1/m, X_2/m, ...$ represents a sequence of random numbers uniformly distributed between 0 and 1, having 'accuracy'

---

[2]Knuth, D.E., The Art of Computer Programming, Volume 2: Seminumerical Algorithms, p. 85, Addison-Wesley, N.Y., 1969.

or 'truncation error' $1/v_n$ with respect to the independence of n consecutive values of the sequence averaged over the entire period."

Equation (1) represents the spectrum of the linear congruential sequence. It can be seen from (1) that $f(s_1,d_2,\ldots,s_n) = 0$ except when

$$s(a) = s_1 + s_2 a + \ldots + s_n a^{n-1} \equiv 0 \pmod{p}$$

in this case $f(s_1,s_2,\ldots,s_n) = 1$. Again directly quoting Knuth[3]:

"...for linear congruential sequences of maximum period, the smallest nonzero wave number in the spectrum is given by

$$v_n = \min\ (s_1^2 + s_2^2 + \ldots + s_n^2)^{1/2}$$

where the minimum is taken over all n-tuples of integers $(s_1,s_2,\ldots,s_n)$ satisfying (2)."

Knuth then proceeds to develop an elaborate computational scheme to implement the spectral test. As with the lattice test algorithm of Ahrens and Dieter, the test algorithm is formulated in terms of the solution to a positive definite quadratic form. To find the minimum value of the wave

---

[3] Ibid., p. 85.

number $(s_1^2 + s_2^2 + \ldots + s_n^2)^{1/2}$ such that $s(a) = s_1 + s_2 a + \ldots + s_n a^{n-1} \equiv 0 \pmod{p}$ the problem may be reformulated as:

find the minimum value of the quantity

$$(a_{11}s_1+a_{12}s_2+\ldots+a_{1n}s_n)^2 + \ldots + (a_{n1}s_1+a_{n2}s_2+\ldots+a_{nn}s_n)^2$$

This results in the positive definite quadratic form

$$(s_1,s_2,\ldots,s_n)' \; A \; (s_1,s_2,\ldots,s_n)$$

where $(s_1,s_2,\ldots,s_n)$ is a column vector, not all zero, and A is any nonsingular matrix of coefficients.

C. THE SPECTRAL TEST IN A FINITE FIELD

The computational algorithm for the spectral test is somewhat more involved than the algorithm for the lattice test. Knuth's algorithm, however, is very carefully written and can very easily be implemented assuming the availability of multiple-precision arithmetic subroutines.

In view of the finite field approach of this thesis, the basic assumptions of the spectral test appear entirely inappropriate. To begin, consider the discrete probabilistic basis of the spectral test. In one dimension, the probability measure assigned to each element is correctly 1/p. However, in higher dimensions, the probability measure for each n-tuple in the space is taken to be $1/p^n$. Since only p distinct

n-tuples are generated by a linear congruential generator, the correct measure should be still 1/p. This point is more clearly seen when it is recalled that all n-tuples generated by a primitive root/prime modulus generator in finite dimensional space are integral multiples of the basic vector $(1,a,a^2,\ldots,a^{n-1})$. That is, the set of all possible n-tuples is

$$\{k(1,a,a^2,\ldots,a^{n-1}) \pmod p\} \ , \quad k = 1,2,\ldots,p-1$$

Similarly, the theoretical basis of the spectral test is the finite Fourier transform defined only in the complex field. When viewing the sequence generated by the primitive root/prime modulus random number generator as a finite field, a more appropriate transform is available, specifically the number theoretic transforms as developed by Rader [Ref. 12], Agarwal and Burris [Ref. 1], and Pollard [Ref. 11]. The finite Fourier transform has been used since in the complex field a primitive root of unity exists, namely $\exp(2\pi ik)$. In finite fields, any primitive root of the prime modulus is a primitive root of unity and consequently a transform (generating function) is defined. For the case of primitive root/prime modulus generators, the spectral test may be more appropriately defined in terms of these transforms.

As in the lattice test, only p possible n-tuples can be generated, hence the search for the minimum value of the wave number $(s_1^2 + s_2^2 + \ldots + s_n^2)^{1/2}$ such that

$s(a) = s_1 + s_2 a + \ldots + s_n a^{n-1} \equiv 0 \pmod{p}$ becomes impossible. The following theorem demonstrates this fact.

Theorem 9: For the primitive root/prime modulus random number generator $X_{i+1} \equiv a\, X_i \pmod{p}$ no solution to the basic congruence

$$s(a) = s_1 + s_2 a + \ldots + s_n a^{n-1} \equiv 0 \pmod{p}$$

exists in the finite field of characteristic p.

Proof: Referring to the development of finite fields in Chapter II and Chapter IV, Section C, the only possible wave in the spectrum of the primitive root/prime modulus random generator must be of the form $k(1,a,\ldots,a^{n-1}) \pmod{p}$ for some integer k such that $0 < k \leq p-1$. Since p is prime, it has no integral divisors, hence $(1+a+\ldots+a^{n-1})$ must be congruent to 0 modulo p. This cannot happen for any n such that $0 < n \leq p-1$. Let n = 1, then

$$(1+a) = 0 \pmod{p}$$

since this implies that a = p-1 or a = -1 in primitive mark notation and ±1 are not, by definition, primitive roots of any prime $p > 2$. Let n = p-1, then

$$(1 + a + \ldots + a^{p-1}) = \sum_{i=0}^{p-1} a^i = 1 - a^p/1-a$$

$$= 1 - a/1-a$$

$$= 1 \not\equiv 0 \pmod{p}.$$

Let $1 < n < p-1$, then

$$(1 + a + \ldots + a^n) = \sum_{i=0}^{n-1} a^i = 1-a^n/1-a \not\equiv 0 \pmod{p}$$

since for this to be congruent to 0 would imply that $a^n \equiv 1$ which contradicts the primitivity of a for which p-1 is the smallest positive integer such that $a^{p-1} \equiv 1 \pmod{p}$. Q.E.D.

The spectral test, when considered as a special case of the lattice test, is still useful when characterizing linear congruential sequences. Unfortunately, the formulation of the test is, at best, shakey. In simpler terms, the spectral test is designed to determine the minimum Euclidean distance between consecutive hyperplanes containing points of the generated sequence. In contrast to the lattice test, only the shortest side of the hypercube is of interest, rather than the ratio of longest to shortest side. The spectral test may be most simply restated for primitive root/prime modulus random number generatros as:
find the minimum value of

$$v_n^2 = k(1^2 + a^2 + \ldots + a^{2(n-1)}) \pmod{p}$$

over all k such that $0 < k \leq p-1$.

As in Chapter IV on the lattice test, this chapter will stop painfully short of producing a general purpose algorithm for a new spectral test. As the conclusions will reiterate, future work will most certainly produce such an algorithm.

VI. CONCLUSIONS

The development of primitive root/prime modulus sequences as finite fields has opened an entirely new perspective on the characterization of congruential random number generators. The results established in the proceeding chapters have been confined to the class of primitive root/prime modulus generators but it is felt that the results are readily extendible to mixed generators with composite moduli.

The lattice test and spectral test have been shown to be equivalent in their power to characterize sequences, the choice of one test over the other is merely a matter of taste. While the theoretical, geometric, and intuitive appeal of both tests are appealing, their implementation has suffered from over-sophistication. The sparse results presented here were worked out by hand calculator. Several other generators have also been examined by hand and the results agree with published lattice test results. Some cases of published results did not work out as simply since the multipliers were greater than the square root of the modulus and the multiplicative inverses, which would have produced the correct results, were too difficult to find.

Further development of the results presented here will lead to criteria for selecting multipliers which will produce nearly optimal properties of the sequence as characterized by the lattice and spectral tests.

The lattice and spectral test algorithms can be redeveloped completely based on finite field properties. The implementation of such algorithms will be quite natural for digital computers since all arithmetic on digital computers is necessarily confined to finite field arithmetic due to the finite capacity of the registers. ("Real arithmetic", or floating point, is confined to a finite set of the rationals.)

The implications of the results presented here are far-reaching. On-going research should bring them to fruition.

BIBLIOGRAPHY

1. Agarwal, Ramesh C. and Burrus, Charles S., "Fast Convolution Using Fermat Number Transforms with Applications to Digital Filtering", IEEE Transactions on Acoustics, Speech, and Signal Processing, v. ASSP-22 no. 2, p. 87-97, April 1974.

2. Ahrens, J.H. and Dieter, U., Uniform Random Numbers, to be published.

3. Ahrens, J.H., Dieter, U., and Grube, A., "Pseudo-Random Numbers a New Proposal for the Choice of Multiplicators," Computing, v. 6, p. 121-138, 1970.

4. Beyer, W.A., Roof, R.B., and Williamson, Dorothy, "The Lattice Structure of Multiplicative Congruential Pseudo-Random Vectors," Mathematics of Computation, v. 25, p. 345-363, 1971.

5. Coveyou, R.R., and MacPherson, "Fourier Analysis of Uniform Random Number Generators," Journal of the Association for Computing Machinery, v. 14, no. 1, January 1967.

6. Franklin, Joel N., "Deterministic Simulation of Random Processes," Mathematics of Computation, v. 17, p. 28-59, 1963.

7. Jansson, Birger, Random Number Generators, Almquist and Wiksell, 1966.

8. Knuth, Donald E., The Art of Computer Programming: Seminumerical Algorithms, Volume 2, Addison-Wesley, 1969.

9. Learmonth, G.P. and Lewis, P.A.W.,

10. Marsaglia, George, "The Structure of Linear Congruential Sequences," in Applications of Number Theory to Numerical Analysis, Zaremba, S.K., Ed., Academic Press, 1972.

11. Marsaglia, George, "Random Numbers Fall Mainly in the Planes," Proceedings of the National Academy of Sciences, v. 61, 1968.

12. Pollard, J.M., "The Fast Fourier Transform in a Finite Field," Mathematics of Computation, v. 25, p. 365-374, 1971.

13. Rader, Charles M., "Discrete Convolutions via Mersenne Transforms," IEEE Transactions on Computers, v. C-21, no. 12, p. 1269-1273, December 1972.

14. Smith, C.S., "Multiplicative Pseudo-Random Number Generators with Prime Modulus," Journal of the Association for Computing Machinery, v. 18, no. 4, p. 586-593, October 1971.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Documentation Center Cameron Station Alexandria, Virginia 22314	2
2.	Library, Code 0212 Naval Postgraduate School Monterey, California 93940	2
3.	Professor P.A.W. Lewis, Code 55Lw Department of Operations Research and Administrative Sciences Naval Postgraduate School Monterey, California 93940	1
4.	Professor. W. Raike, Code 55R Department of Operations Research and Administrative Sciences Naval Postgraduate School Monterey, California 93940	1
5.	Mr. G. P. Learmonth 2829 Carlton Drive Ann Arbor, Michigan 48104	1