Hull, T.E. and A.R. Dobell
"Random Number Generators."
SIAM Review 4.3 (1962) 230-254.

SIAM REVIEW
Vol. 4, No. 3, July, 1962

RANDOM NUMBER GENERATORS[1,2]

T. E. HULL[3] and A. R. DOBELL[4]

1. SUMMARY

A NUMBER OF TECHNIQUES IN APPLIED MATHEMATICS AND STATISTICS involve what are called Monte Carlo calculations. Such calculations depend on having available sequences of numbers which appear to be drawn at random from particular probability distributions. For convenience we will refer to any such numbers simply as random numbers.

Our purpose is to survey the problem of obtaining these sequences of numbers, with particular emphasis on the procedures used for their generation on stored-program computers. The term "pseudo-random" is often used to describe the random numbers which are obtained on computers.

We begin in section 2 with a brief indication of what types of calculations require such a supply of random numbers.

Then in section 3 we turn to the main topic, which is a thorough treatment of the number theoretic properties of the methods of generation called "mixed congruential", followed for comparison by a brief treatment of the older "multiplicative congruential" methods. We find that the former have several theoretical advantages over the latter. We also refer briefly to some recent theoretical results concerning the serial correlation of the generated sequences.

In section 4 we consider some of the statistical properties which must also be required of these sequences. Here the mixed methods lose some of their attractiveness. Under certain circumstances they can produce sequences which fail to pass the required tests. On the other hand the multiplicative methods produce sequences with consistently good statistical properties.

In the final three sections we summarize other aspects of the subject. In section 5 we consider the problem of using numbers from the uniform distribution to obtain numbers from various other distributions. In section 6 we draw attention to several problems which seem to warrant further study. Finally, in section 7, we describe some of the historical development of the subject, and here we refer to other methods, and to other approaches to the problem.

The bibliography is intended to be complete with respect to references concerned with the generation of random numbers on computers. It contains substantially all such references to the open literature, as well as many references to government and company reports. In addition it contains a number of references concerning each of the related topics which are considered in this paper.

2. CALCULATIONS REQUIRING RANDOM NUMBERS

Random numbers are required in a wide variety of both commercial and scientific calculations. The term "Monte Carlo" is now commonly applied to any

[1] Received by the editors April 5, 1962.
[2] This work was supported in part by the National Research Council of Canada.
[3] University of British Columbia.
[4] University of British Columbia; now at Massachusetts Institute of Technology.

calculation involving such numbers. The term was used first in 1946, in connection with a procedure developed by von Neumann and Ulam at Los Alamos [104]. Since then there has been a considerable growth of interest in Monte Carlo techniques, primarily because their potential has been so tremendously increased with the use of high-speed computers.

Some types of calculations involve the use of random numbers in a natural way. For example, this is the case if one is following the path of a neutron or some other particle which is subjected to random collisions. Other examples occur in statistics, in the study of queues, in games of strategy, and in other competitive enterprises. In all these situations the randomness is inherent, and the calculations are simulations of the corresponding physical processes. Many examples of calculations of this sort will be found in the proceedings [83] of a symposium held at the University of Florida in 1954. An extensive bibliography, having abstracts with most of the references, has been added to these proceedings as an appendix. More recently a survey has been given by Bauer [4]. Nuclear reactor calculations are discussed by Richtmyer [104]. Applications to random walk problems are described in a book by Cashwell and Everett [15]. A unified approach to Monte Carlo methods for particle transport problems is presented by Spanier [113]. An interesting discussion of the general theory has been given by Hammersley [50]. Of course many other papers on individual problems have also appeared in recent years, in the social and in the life sciences, as well as in the physical sciences.

Other types of calculations involve the use of random numbers in a much less natural way. Usually the situation is as follows. One requires a particular number which is the answer to some completely deterministic problem, such as the value of some definite integral $\int_0^1 f(x)\,dx$, where $0 \leqq f(x) \leqq 1$. One then sets up a stochastic process with the property that the expected value of some random variable is the required number, and estimates this expected value on the basis of some (more or less sophisticated) sampling procedure. In the case of our integral, the process could be simply the drawing of two numbers a and b from the uniform distribution on the interval $[0, 1)$. The random variable which is 1 if $f(a) \leqq b$, and 0 otherwise, has the required expected value.

Such stochastic processes have also been proposed for the solution of differential and integral equations, for the finding of eigenvalues, and for the inversion of matrices. See particularly the bibliography in the proceedings [83] referred to above. A general theory has been discussed by Curtiss [20]. Experiments in computing multiple integrals have been carried out by Davis and Rabinowitz [21], while partial differential equations have been investigated by Ehrlich [25], and by Todd [125]. Several algorithms are presented in a book edited by Ralston and Wilf [99].

Generally speaking, Monte Carlo methods have not been particularly successful when applied to these less natural situations. However, they are indispensable in most of the natural applications, where there is often no alternative procedure.

A characteristic of the Monte Carlo method is that the required solution is approached with an error which is $0(n^{-1/2})$, where n is the number of trials, or the number of elements in the sample. This means that each additional decimal digit in the result requires 100 times as much computing as the preceding one required. Ordinarily, then, one does not expect more than one or two significant digits in the result. Convergence can often be improved (although the $-\frac{1}{2}$ power of n cannot be changed) by standard variance reducing techniques such as importance sampling. See, for example, the papers by Kahn [60] and by Marshall [79] at the Florida symposium; also [17, 18, 59].

3. THEORETICAL CONSIDERATIONS

To handle the sort of problem we have mentioned briefly in the preceding section we would require sequences of numbers which at least *appear* to be drawn at random from certain probability distributions. The distributions may be uniform, normal, Poisson, or some other. In section 5 we will indicate several ways in which a sequence from any such distribution can be obtained, once we have a sequence from the uniform distribution. Until then we will restrict our attention to sequences of numbers which might appear to be drawn from a uniform distribution.

There are many ways of generating such sequences. In this section we will concern ourselves only with the particular procedures which seem to be best for use on a stored-program computer. Our main objective will be to establish their basic number theoretic properties, and our results are summarized in the two theorems of this section. A second objective is to describe one other theoretical result which has recently been obtained. Questions concerning the statistical properties of our sequences will be dealt with in the next section.

The computing scheme which defines the procedures is as follows. We begin with a positive integer x_0, called the starting value, an integer a, called the multiplier, and another integer c. We also need a fourth integer m, called the modulus, which is positive and greater than the other three in magnitude. We then define a sequence $\{x_i\}$ of non-negative integers, each less than m, by means of the congruence relation

$$x_i \equiv ax_{i-1} + c \pmod{m}. \tag{1}$$

Finally, to obtain numbers in the interval [0, 1), we form the sequence $\{x_i/m\}$.

Of course any sequence generated in this way is completely determined in advance, and could hardly be called "truly random". However, for many values of the parameters defining such sequences, the resulting numbers might well seem to be quite haphazardly taken from the interval [0, 1). The extent to which they do appear to be drawn at random from the uniform distribution on this interval will be our concern in the next section. It turns out rather surprisingly that the statistical behavior of our sequences is good, with only a few exceptions, as long as they do not repeat too soon. We will therefore first concentrate on making sure that our sequences do not repeat too soon.

Now it is clear that any sequence must repeat itself eventually, because it can contain at most m different numbers, each number in a particular sequence being determined solely by its predecessor. It happens to be quite easy to ensure that we have the full period m in the general case, and to ensure that we have very nearly the full period in the important special case defined by $c = 0$. Our two theorems will therefore prescribe conditions on x_0, a, m, and, in the general case, c, which will ensure maximum possible period.

We should point out that in practice we usually find it desirable to choose m to be a power of 2 on a binary machine, or a power of 10 on a decimal machine. We are then able to avoid the division which is implicit in the congruence, and also the division to form x_i/m. Other choices are possible and will be referred to later. However, we can ordinarily take m as given, and then our problem is to find what choice of x_0, a, and possibly c, will ensure a maximum period.

The general case in which we do not require c to be zero is the simpler of the two and will be treated first. It appeared in 1960 in papers by Coveyou [19] and Rotenberg [107]. A more recent treatment has been given by Greenberger [41, 42] and by Peach [97]. The method has also been tested by Kuehn [66]. A quite different approach to the essential idea had been given by Thomson [120] in 1958.

The basic theorem is the following.

THEOREM 1. *The sequence defined by the congruence relation* (1) *has full period* m, *provided that*

(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.

Thus with m a power of 2, as is natural on a binary machine, we need only have c odd, and $a \equiv 1 \pmod 4$. With m a power of 10 we need only have c not divisible by 2 or 5, and $a \equiv 1 \pmod{20}$.

For the proof of this theorem we first point out that when $a = 1$, and c is relatively prime to m, the period is obviously m. We therefore need consider only the case $a \not\equiv 1$, which we will henceforth assume.

Using (1) with $i = 1, 2, \cdots, n - 1$, we easily obtain

$$x_n \equiv a^n x_0 + \frac{(a^n - 1)c}{a - 1} \pmod m.$$

and we are interested in the smallest value of n such that $x_n = x_0$, that is, such that

$$\frac{(a^n - 1)(x_0(a - 1) + c)}{a - 1} \equiv 0 \pmod m.$$

By the conditions of the theorem, $x_0(a - 1) + c$ is relatively prime to m. Thus we are interested in the smallest value of n such that

$$(a^n - 1)/(a - 1) \equiv 0 \pmod m. \tag{2}$$

We want to show that this smallest value of n is equal to m, provided the multiplier a satisfies the conditions of the theorem.

We will first prove this result for $m = p^\alpha$, where α is a positive integer, and p is an odd prime. When $\alpha = 1$ condition (ii) leads us again to the trivial case with $a = 1$. We therefore need only consider $\alpha \geqq 2$.

Because a satisfies the conditions of the theorem and $a \neq 1$, we can put

$$a = 1 + kp^{\beta}, \tag{3}$$

where k is relatively prime to p and $k \neq 0$, and where β is a positive integer.

To see that $n = p^{\alpha}$ satisfies (2), we substitute this value of n into the left side of (2), along with the expression (3) for a. We easily obtain

$$\frac{a^n - 1}{a - 1} = p^{\alpha} + \frac{p^{\alpha}(p^{\alpha} - 1)}{1 \cdot 2} kp^{\beta} + \frac{p^{\alpha}(p^{\alpha} - 1)(p^{\alpha} - 2)}{1 \cdot 2 \cdot 3} (kp^{\beta})^2 + \cdots + (kp^{\beta})^{p^{\alpha}-1}. \tag{4}$$

We have to prove that this expression is divisible by p^{α}. In fact it turns out that each term in this expression is divisible by p^{α}. To see that this is the case we rewrite the jth term as follows

$$\frac{p^{\alpha}}{j}\left[\frac{(p^{\alpha} - 1)(p^{\alpha} - 2) \cdots (p^{\alpha} - j + 1)}{1 \cdot 2 \cdots (j - 1)}\right] k^{j-1}p^{(j-1)\beta}, \qquad (j > 1).$$

The part of this term which precedes the factor k^{j-1} is a binomial coefficient, and is therefore an integer. Each factor in the denominator of this part must therefore divide into the numerator of this part. But the part in square brackets is also a binomial coefficient, and hence an integer. Therefore j is the only factor in the denominator which, on dividing into the numerator, might "need" any of the factor p^{α} in the numerator. However the number of times the factor p can appear in j is less than

$$\frac{j}{p} + \frac{j}{p^2} + \frac{j}{p^3} + \cdots = \frac{j}{p - 1}, \tag{5}$$

and is therefore less than or equal to $j - 1$. But the factor p appears at least this many times in $p^{(j-1)\beta}$, since $\beta \geqq 1$. Thus the factor p^{α} is not needed at all to enable j to divide into the numerator. Every term on the right side of (4) is therefore divisible by p^{α}. This means that (2) is satisfied by $n = p^{\alpha}$, at least under the stated conditions.

We must now show that no value of n *smaller* than p^{α} will satisfy (2). It is easy to show that a value of n will satisfy (2) if and only if it is a multiple of the smallest such value; we use the idea in Ore [92, p. 280]. Knowing that $n = p^{\alpha}$ does satisfy (2), we therefore need to consider only values of n which are powers of p. Indeed it is sufficient for our purposes to show that $n = p^{\alpha-1}$ does *not* satisfy (2).

Substituting $n = p^{\alpha-1}$ into the left side of (2), along with the expression (3) for a, we now obtain

$$\frac{a^n - 1}{a - 1} = p^{\alpha-1} + \frac{p^{\alpha-1}(p^{\alpha-1} - 1)}{1 \cdot 2} kp^{\beta} + \frac{p^{\alpha-1}(p^{\alpha-1} - 1)(p^{\alpha-1} - 2)}{1 \cdot 2 \cdot 3} (kp^{\beta})^2 + \cdots + (kp^{\beta})^{p^{\alpha-1}-1}.$$

We will show that the right side is *not* divisible by p^{α}. The first term is obviously not divisible by p^α, and so it will be sufficient to show that each of the other terms is divisible by p^α. The argument follows exactly the one given above for the jth term in (4), except for one small change. This time we have $p^{\alpha-1}$, instead of p^α, appearing as a factor in the binomial coefficient. We need another factor p. This other factor is to be found in $p^{(j-1)\beta}$ *provided* we now make use of our assumption that p is odd, in which case (5) is less than or equal to $j - 2$, instead of $j - 1$.

We have now completed the proof of the theorem when $m = p^\alpha$, and p is odd. The proof when $m = 2^\alpha$ is only slightly different. The case where $\alpha = 1$ is again trivial. The case where $\alpha \geqq 2$ differs from the above in that in (3) the positive integer β must now be greater than 1. This restriction on β is needed only in the last sentence of the proof which would become: "This other factor is to be found in $p^{(j-1)\beta}$ *provided* we now make use of our assumption that $\beta > 1$."

Now that the theorem is established when m is restricted to being a power of a prime, it is quite easy to generalize to the case where m is composite. In fact we simply put

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}, \qquad a = 1 + k p_1^{\beta_1} p_2^{\beta_2} \cdots p_s^{\beta_s},$$

with p_i prime, α_i a positive integer, $k \not\equiv 0$ and relatively prime to m, $\beta_i \geqq 1$ or, if $p_i = 2$ and $\alpha_i \geqq 2$, $\beta_i \geqq 2$. Then the argument proceeds almost exactly as before, and the theorem is established in the general case.

Before considering the merits of the random number generators suggested by the above theorem, we will consider briefly another class of generators. These others are obtained from (1) by taking $c = 0$, and are sometimes called multiplicative congruential methods. They are also called power residue methods because, if we take x_0 to be relatively prime to m, we are led to

$$a^n \equiv 1 \pmod{m} \tag{6}$$

in place of (2). We are no longer able to choose a so that our sequence has full period m. We can, however, choose a so that the period is still quite large.

The generators so obtained are the most widely used at the present time. The basic idea was introduced in 1949 by Lehmer [67]. In section 7 we will give more details of his special version. The version which is usually used has been discussed and tested by many authors including Bofinger and Bofinger [5], Certaine [16], Duparc, Lekkerkerker and Peremans [23], Gilbert [34], Hamming [51], Juncosa [58], Matteis and Faleschini [80], Meyer, Gephart and Rasmussen [84], Orcutt, Greenberger, Korbel and Rivlin [91], Taussky and Todd [118], and in an IBM report [56]. Such generators are also described in the surveys of Edmonds [24], Golenko [35], Page [94], Teichroew [119], Tocher [124], Votaw and Rafferty [134], and in a popular account by Spenser [114]. Only the decimal case is considered by Moshman [85], while only the binary case is considered by Barnett [1], and Johnson [57]. Barnett corrects an error in a paper by Leslie and Gower [69],

The basic theorem for the multiplicative congruential methods is more complicated and more difficult than for the mixed congruential methods. Because of this, and because special cases of the theorem have already appeared in a number of the above papers, we will merely summarize the proof for the general case. For the details we will refer to standard results in number theory, as given for example by Ore [92, ch. 12].

We want to describe conditions on a which will ensure that the smallest value of n satisfying (6) is a maximum. This value of n is sometimes called the *indicator* of m, and will be denoted by $\lambda(m)$. Any corresponding number a is said to *belong* to the indicator.

We will reach the theorem in two stages. We first consider m to be composite

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s},$$

where the p's are distinct primes. Then it is fairly easy to show [92, p. 293] that

$$\lambda(m) = \text{l.c.m.}\ (\lambda(p_1^{\alpha_1}), \lambda(p_2^{\alpha_2}), \cdots, \lambda(p_s^{\alpha_s})),$$

and that it is sufficient to have a belong simultaneously to each $\lambda(p_i^{\alpha_i})$. Moreover it is a consequence of a theorem called the Chinese Remainder Theorem that there do exist such values of a [92, p. 294].

We therefore have only to consider the case where m is the power of a prime, say p^α. But then the problem is a very well-known one in number theory. If p is odd it turns out that the indicator $\lambda(p^\alpha) = (p - 1)p^{\alpha-1}$, and the corresponding values of a are the primitive roots for p^α [92, pp. 284–288]. The result depends in part on a famous theorem of Euler's [92, p. 273]. It is in general extremely tedious to find primitive roots, but we will shortly describe a simple procedure which is sufficient for our purposes.

If $p = 2$ we have primitive roots only when $\alpha = 1$ (root is 1), and $\alpha = 2$ (root is 3). For other values of α it turns out that $\lambda(2^\alpha) = 2^{\alpha-2}$, and 3 is a value of a belonging to this indicator. See [92, pp. 288–290]. It can also be shown that, for $\alpha > 2$, it is necessary and sufficient that $a \equiv \pm 3 \pmod 8$. For example, see [41].

We can summarize the main properties of multiplicative congruential methods in the following theorem.

THEOREM 2. *The sequence defined by taking* $c = 0$ *in the congruence relation* (1) *has maximal period, provided that*

(i) x_0 *is relatively prime to* m;

(ii) a *is a primitive root for* p^α, *if* p^α *is a factor of* m, *with* p *odd and* α *as large as possible, or with* $p = 2$ *and* $\alpha = 1$ *or* 2;

(iii) a *belongs to* $2^{\alpha-2}$, *if* 2^α *is a factor of* m, *with* $\alpha > 2$. *Moreover, for any* m, *there exist values of* a *satisfying these conditions, and, finally, the maximal period is the lowest common multiple of the periods,* $(p - 1)p^{\alpha-1}$ *or* $2^{\alpha-2}$, *with respect to the prime power factors.*

In practice it is easy to satisfy condition (i). By insisting that $a \equiv \pm 3 \pmod 8$ we can also satisfy (iii).

We still need a simple way to find primitive roots of prime powers when the prime is odd. One such way depends on the following result [92, p. 285–288]: if r is a primitive root for p, and if $r^{p-1} = 1 + tp$ where t is not divisible by p, then r is a primitive root for p^α. Moreover it is easy to see that if r satisfies the stated conditions then so will any number which is congruent to $r \pmod{p^2}$.

Consider the case with $p = 3$. Here it is easy to verify that 2, 5, 8 are primitive roots for 3. It is also easy to verify that 2 and 5 satisfy the second condition required of r, while $8^{3-1} = 1 + (21)3$, and so 8 does not. We conclude that, for ternary machines with word length α, we will obtain maximum period $2(3^{\alpha-1})$ provided we choose x_0 to be not divisible by 3, and a $\equiv$ (2 or 5) (mod 9).

For the case $p = 5$, it is a straightforward matter to verify that the primitive roots are congruent to 2 or 3 (mod 5), and that it is sufficient to choose $a \equiv (2, 3, 8, 12, 13, 17, 22, \text{ or } 23) \pmod{25}$.

For a decimal machine with word length α we can use the theorem to combine the effects of the factors 2^α and 5^α. We take x_0 to be any number not divisible by 2 or 5. Then, for $\alpha = 1$ we obtain the maximum period 4 by taking $a = 3$ or 7. For $\alpha = 2$ the maximum period is 20 and we can take $a = 3, 23, 27, 47, 63, 67, 83, 87$. For $\alpha = 3$ the maximum period is 100, while for $\alpha \geqq 4$ it is $5(10^{\alpha-2})$. For $\alpha \geqq 3$ we can take $a \equiv \pm (3, 13, 27, 37, 53, 67, 77, \text{ or } 83) \pmod{200}$.

Perhaps we should emphasize that the conditions on a are sufficient, but by no means necessary. In fact for the decimal machine with $\alpha \geqq 3$ it is also sufficient to take $a \equiv \pm (19, 29, 59, \text{ or } 69) \pmod{200}$ for which the periods are only $2(5^{\alpha-1})$, relative to the modulus 5^α alone. It is even sufficient to take $a \equiv \pm (11, 21, 61, \text{ or } 91) \pmod{200}$ for which the periods are only $5^{\alpha-1}$, relative to 5^α alone.

Of the references on the multiplicative method which we have already mentioned, the IBM report [56] and the report of Matteis and Faleschini [80] give the most complete prescriptions for choosing the multiplier a. Other authors have needed only a suitable value or two, and have sometimes presented a simple rule for choosing a. For example, a common rule for binary machines is to choose a to be an odd power of 5, such as 5^{13}. It is easily shown that any such $a \equiv -3 \pmod 8$. For decimal machines it is often suggested that a be a power of 3, where the power is relatively prime to 10, as in 3^{17}. It can be shown that such a multiplier will ensure maximum period.

Let us now consider the relative merits of the mixed and multiplicative congruential methods. On the basis of the theoretical evidence obtained so far, it appears that the mixed have several small advantages over the multiplicative.

The methods can both be made quite fast by choosing multipliers which are easily effected by "shift-and-add" operations. For example, with the mixed methods, we can use $2^\alpha + 1$ on a binary machine, or $10^\alpha + 1$ on a decimal machine. One shift, and one add operation is needed in each case, followed by the addition of c. The simplest choice with the multiplicative methods is $2^\alpha + 3$, or $10^\alpha + 3$, which in either case will involve one more operation. Incidentally such "shift-and-add" procedures will leave the multiplier-quotient register unchanged.

The mixed methods also of course have longer periods. But the periods are in either case extremely long, so this is not usually a real advantage. A case where it could be an advantage arises if one is using a computer with a variable word length. Then with the mixed methods one could use a shorter word length, for the period required, and consequently save on multiplication, or addition time.

In some calculations we may want to use individual digits of our random numbers as random digits. With multiplicative methods only the most significant digits have the maximum period, the other digits having periods which are progressively smaller as their significance decreases. Statistical evidence from some of the papers referred to in the next section indicates that only the first few digits can be relied upon. The situation is probably better with the mixed methods, although this point has not yet been investigated thoroughly.

One final advantage of mixed methods lies in their relative simplicity. The basic theorem is much easier to establish, and the conditions are much easier to remember.

The only disadvantage of mixed methods is in their statistical behavior. Their behavior in this respect is generally very good, but some cases are completely unacceptable. These cases constitute only a small fraction of the total, but there are no such cases among the multiplicative methods.

Before considering the statistical properties any further, there is one more theoretical aspect of the problem which should be described.

In the past, almost all theoretical work on random number generators has been concerned with number theoretical properties of the sequences generated, and in particular with period lengths. Very recently Coveyou [19] and Greenberger [41, 42] introduced some theoretical results of an entirely different nature. They calculated the serial correlation coefficient for a sequence with full period. The purpose was to show how this correlation coefficient depends on the parameters involved; in this way we are led to choosing those parameters so that, besides having a long period, we also have a small serial correlation in the sequence generated.

The most general expression for the serial correlation ρ is given by Greenberger [42]. It is

$$\rho \approx \frac{1}{a} - \frac{6c}{am}\left(1 - \frac{c}{m}\right) + K,$$

where it can be shown that $-a/m \leqq K \leqq a/m$. Greenberger points out that very small or very large values of a are to be avoided. He also points out that values of a near to $m^{1/2}$ will yield small values of ρ, regardless of the value of c, and he gives details for a number of special cases.

The above result is for a serial correlation of lag 1. Both Coveyou and Greenberger point out that correlations of lag k, for $k > 1$, can be obtained from the above. They show that the sequence consisting of every kth member of the original sequence is itself a sequence of the form (1), but with multiplier a^k, and additive constant $(a^k - 1)c/(a - 1)$; both parameters should of course be calculated "mod m".

4. STATISTICAL TESTS

Having completed a theoretical investigation of both the mixed congruential and the multiplicative congruential methods of random number generation, we now turn our attention to a study of their behavior from a statistical point of view.

Our purpose all along has been to obtain sequences of numbers which can be considered to be drawn at random from a uniform distribution. The key phrase here is "can be considered to be". We know our numbers are *not* drawn at random from a uniform distribution, but for practical purposes it is sufficient that they have the *appearance* of being so drawn. This is of course not the first time in life where we meet a situation in which it is only the appearance of what we are doing that matters!

Our congruential methods are completely deterministic. Our hope is that we will nevertheless be able to use them to simulate a random process. As a matter of fact the situation is not so very different from "random processes" like the rolling of dice. At least from the point of view of Newtonian mechanics the rolling of dice is completely deterministic. Nevertheless much of what happens is adequately described by a probabilistic model.

Whether or not a set of numbers appears to have come from a particular distribution is a standard question for statistical techniques. Many tests have been devised and studied. When one does not have in mind any alternative to the particular distribution being considered, it is quite natural to use the well-known χ^2 test on some particular property of the distribution.

For example, it is natural to require our sequence of numbers to be uniformly distributed over the interval [0, 1). To test them for this property we can divide the interval into a number of equal sub-intervals. We could use 10 sub-intervals with decimal arithmetic, perhaps 8 with binary arithmetic. The frequency f_i, or the number of numbers in the ith interval, can then be obtained for a sequence of numbers. We then compute the statistic

$$\chi_1^2 = \frac{k}{n} \sum_{i=1}^{k} \left(f_i - \frac{n}{k}\right)^2$$

where n is the length of the sequence, and k is the number of sub-intervals. It is well-known that this statistic has, for large n, a χ^2 distribution with $k - 1$ degrees of freedom. This means, for $k = 10$ for example, that this statistic would be expected to exceed 16.9 with probability only 5%, provided the sequence is actually drawn at random from the uniform distribution.

One could also compare sample moments with those expected from the uniform distribution. These tests are like the frequency test just described in that they do not depend on the *order* in which the numbers are generated.

Another class of tests does depend on the order. Perhaps the best known of these, at least in this context, is the serial test. We can define this test by first letting f_{ij} be the number of numbers in the ith interval which are followed by a number in the jth interval. Then we compute

$$\chi_2^2 = \frac{k^2}{n} \sum_{i,j=1}^{k} \left(f_{ij} - \frac{n}{k^2}\right)^2.$$

It was shown by Good [38, 39] that $\chi_2^2 - \chi_1^2$ has asymptotically a χ^2 distribution with $k^2 - k$ degrees of freedom, and also that $\chi_2^2 - 2\chi_1^2$ is asymptotically χ^2 with $(k - 1)^2$ degrees of freedom.

The frequency test and the serial test were proposed in two well-known papers by Kendall and Babington-Smith [61, 62], although they had in mind tests for certain sequences of digits, rather than sequences of numbers. They also proposed a "poker test", and a "gap test". These papers appeared in 1938 and 1939, which was long before arithmetic processes were used in the generation of random numbers. The tests, especially the first two, are still widely used. However the correction by Good, of their statistic for the serial test, should be noted [38, 39], as has been pointed out by Tompkins [127].

At about the time of the Kendall and Babington-Smith papers there also appeared related papers by Nair [89], Yule [142], and Kermack and McKendrick [64, 65]. The latter introduced tests based on the expected occurrence of runs in a random sequence. An error in their procedure has been pointed out by Levene and Wolfowitz [70]. For examples of tests introduced in the early 1940's, reference should also be made to Dodd [22], to Gage [32], to Rosander [106], and to Swed and Eisenhart [117].

In 1950 Gruenberger [45] gave a brief description of the tests proposed by Kendall and Babington-Smith. Since then a number of other tests have been proposed. Gruenberger and Mark [46] proposed a "d^2 test" which was designed to test the suitability of random numbers as spatial coordinates in certain Monte Carlo calculations. Later there appeared a "coupon collector's test" by Greenwood [43], a "partition test" by Butcher [10], and a test for grouping by Wall [136]. The standard tests along with a number of variants are also described in most of the references which were given in section 3.

For completeness we also mention a test for repeating cycles given by Hunter [55], but this test has nothing to do with the randomness itself.

Of course tests for randomness are of interest apart from the context of random number generators, and there are many references on the subject. The most important source is probably the Annals of Mathematical Statistics.

The term "pseudo-random" is often used to describe sequences of numbers which are able to pass tests for randomness, even though the sequences may have been generated by a completely deterministic process. In this way one may avoid becoming involved in any philosophical arguments about the meaning of randomness, arguments which, according to Kendall and Babington-Smith [61], are "of an abstract metaphysical character bordering at times on the theological". One may even avoid being accused of immorality! Indeed, von Neumann [133] stated that anyone who uses arithmetical methods to produce random numbers "is, of course, in a state of sin".

Lehmer [67] described a pseudo-random sequence as "a vague notion embodying the idea of a sequence in which each term is unpredictable to the uninitiated and whose digits pass a certain number of tests, traditional with statisticians and depending somewhat on the uses to which the sequence is to be put".

We have already stated that the multiplicative methods behave well statistically. Most of the references on these methods given in section 3 include the results of tests, and there are no examples reported of unsatisfactory behavior. We could add the favorable reports by Cameron [13], Forsythe [29], and a more recent one by Sobol' [111]. Information referred to in an abstract by Cameron [14] is summarized by Taussky and Todd [118].

Our own experience confirms this conclusion. We computed both χ_1^2 and χ_2^2 for blocks of 1024 numbers, using eight equal sub-divisions of the interval $[0, 1)$. The results for 100 consecutive blocks were compared with the expected distribution of χ^2 values; here we divided the interval $[0, \infty)$ into percentiles, and calculated one χ^2 statistic for the χ_1^2 values, and another for the χ_2^2 values. The procedure was repeated for 513 different multipliers. We were using a binary machine with $\alpha = 35$, and we took $x_0 = (377777777777)_8$, while the multipliers were $a = (376003)_8 + (10)_8 S$, $S = 0, 1, 2, \cdots, 512$. These multipliers are near to $m^{1/2}$. The results were entirely consistent with the hypothesis that the sequence was drawn at random from the uniform distribution.

The mixed congruential methods are much newer and experience with them has been reported in only a few cases. Rotenberg [107] reports satisfactory results with a very short sequence (4096 numbers) using $a = 2^7 + 1$ with $\alpha = 35$. Kuehn [66] has had success with 500,000 numbers using $a = 2^9 + 1$ with $\alpha = 47$. On the other hand Peach [97] has found evidence of some undesirable patterns, although he obtained satisfactory statistical results with over 250,000 numbers using $a = 2^{11} + 1$ with $\alpha = 28$.

Our own experience using mixed generators has been with a decimal machine, usually with $x_0 = 0$, $c = 1$, and $\alpha = 10$. Again we performed tests on the distribution of the values of χ_1^2 and χ_2^2 for 100 consecutive blocks. This time each block consisted of 1000 numbers, and we used 10 equal subdivisions of the interval $[0, 1)$.

We performed tests on more than 600 different multipliers. We believe that about 1 percent of all possible multipliers may be completely unacceptable, in the sense that they lead to values of χ^2 which are ridiculously large. (We found some as large as 900.) While not complete, the evidence indicates strongly that any multiplier which is unacceptable in this sense, must be congruent to 1 (mod 500). Of those that were not acceptable, some became acceptable when we used more complicated values of c. Others were found to have failed because the χ^2 values for the individual blocks were too nearly the same, although the individual blocks themselves would have been considered quite acceptable.

We were of course interested in simple multipliers, especially those which could easily be effected by "shift-and-add" instructions. For example, the multiplier $10^5 + 1$ was unacceptable, and was not sufficiently improved with more complicated values of c. On the other hand $10^3 + 1$ was acceptable, even with $c = 1$.

It should be emphasized that our criterion for acceptance has been quite arbitrary. Passing tests like the frequency test and the serial test would be considered necessary in most applications, but hardly sufficient. The difficulty is to choose tests which reflect the requirements of the problem to be solved. In a private communication, R. R. Coveyou refers to experiences in which special correlation within a sequence has caused erroneous results in Monte Carlo calculations, in spite of the fact that routine statistical tests did not reveal the existence of such correlation. He draws attention to the need for more quantitative information about the reliability of tests.

Another approach which suggests itself is to use sample problems on which to test Monte Carlo techniques. We have already referred to the experiments on multiple integration by Davis and Rabinowitz [21], and to the work on partial differential equations by Ehrlich [25], and by Todd [125]. The techniques have received further confirmation in an interesting study by Bazley and Davis [3] of the game of Chutes and Ladders. Several other examples are given by Todd [126].

5. NON-UNIFORM DISTRIBUTIONS

So far we have been concerned only with the generation and testing of numbers which appear to be uniformly distributed. This restriction of our interest is justifiable because, in principle at least, it is easy to obtain any other distribution from the uniform distribution. For one dimensional distributions we need only solve the equation $x = F(y)$ for y, where x is uniformly distributed, and where F is the required (cumulative) distribution function.

For example, if y is to be normally distributed, with mean 0 and variance 1, we have

$$x = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} e^{-u^2/2}\, du, \qquad -\infty < y < \infty.$$

Another example of interest is given by

$$x = 1 - e^{-y}, \qquad 0 \leqq y < \infty. \tag{7}$$

One could of course tackle the problem directly by entering a table of values of $F(y)$ to find y for a given x. For example see Lytle [72]. Storage requirements on a computer would be prohibitive with this direct approach, if many significant digits were required.

Alternatively one might try to find an expression giving y in terms of x, or at least an approximation to y in terms of x. The first extensive results in this area were given by Teichroew in his thesis in 1953 [119]. To obtain normal deviates he first takes a sum of a fixed number of uniform deviates. By the Central Limit Theorem this sum is approximately normally distributed. A Chebyshev polynomial is then used to improve this approximation. The relevant parts of his thesis are summarized in a book edited by Solomon [112].

Different Chebyshev approximations over different intervals are used by Muller [86] to obtain the normal distribution. A rational approximation is used by Juncosa [58].

The normal distribution has also been considered by Butcher [11], by Leslie and Gower [69], and by Page [94]. Muller [87] describes and compares a number of procedures for generating normal deviates, including a particularly attractive one by Box and Muller [8].

Marsaglia [75, 76, 77, 78] has recently developed an alternative approach. His approximations are in two parts. One part, consisting of the superposition of a number of simple distributions, is computed most of the time. The other part is quite complicated, but it rarely need be computed.

Thus Marsaglia's method depends on expressing y in the form $a f_1(x) + b f_2(x)$, approximately, where $a \gg b > 0$, $a + b = 1$, and f_1 is simple. The approximations are to be found by computing $f_1(x)$ with probability a, and $f_2(x)$ with probability b.

Wendel [139] points out that we can avoid extracting roots to obtain y, where $F(y) = y^5$, $0 \leqq y < 1$. We need only take y to be the maximum of five independent values of x from the uniform distribution on $[0, 1)$.

A quite different approach was introduced by von Neumann [133] in 1951. It involves an acceptance-rejection technique, which we will illustrate by stating one of the results established by von Neumann. To obtain a sequence of numbers which appears to be drawn from the distribution in (7), we proceed as follows. We choose a sequence of numbers $x_1, x_2, \cdots$ from the uniform distribution. There is a smallest n for which $x_1 > x_2 > \cdots > x_n$ while $x_n \leqq x_{n+1}$. If this n is odd we accept $y_1 = x_1$. But if this n is even, we choose another sequence. If the next n is odd we accept $y_1 = x_1 + 1$ where now x_1 is the first number in the new sequence. But if this second n is also even, we again repeat. We keep repeating the process until we obtain an n which is odd, say on the ith attempt. Then we accept $y_1 = x_1 + i - 1$ where x_1 is the first number of the ith attempt. We then start all over again to find y_2, and so on for $y_3, y_4, \cdots$.

A general discussion of the acceptance-rejection technique, and others, is given by Butler [12], who refers to von Neumann's paper, and to another by Votaw and Rafferty [134]. Clark and Holz [18] give detailed proofs in the case of the above exponential distribution, along with an extensive table. See also Golenko [35], and Kahn [59]. The latter is not readily available, but it does contain a very extensive treatment of the problem of non-uniform distributions, including the idea exploited by Marsaglia, and many applications of acceptance-rejection techniques.

A somewhat different problem, of interest in combinatorial situations, is that of generating random permutations. Here one would like to associate a particular permutation of a fixed number of integers $1, 2, \cdots, n$, with each of $n!$ distinct numbers. For example, if $n = 3$ and our machine is a decimal machine, we could examine only the most significant digit in each random number. Our 6 permutations could then be associated with 0, 1, 2, 3, 4, 5, while random numbers beginning with 6, 7, 8, or 9 would be ignored. The general "association" problem has been considered in detail by Lehmer [68] along with some related questions. See also Tompkins [129], and Rao [101].

Another problem of importance is that of generating points which are uniformly distributed on an N-sphere. For an efficient way of deriving such a sequence from numbers which are uniformly distributed on $[0, 1)$, see Muller [88].

For the generation of correlated numbers see Pakov [95].

6. FURTHER CONSIDERATIONS

In this section we want to draw attention to several areas in which there seems to be a need for further research.

More results are needed in the area recently opened up by Coveyou [19] and

Greenberger [41, 42], and already referred to at the end of section 3. Here the problem is to determine theoretically the way in which various statistical properties of the generated sequences depend on the parameters. One might then learn how to choose these parameters so as to ensure good statistical properties of the sequences, as well as ensuring sufficiently long periods.

This immediately raises another important question. What do we mean by good statistical properties? Just passing a fixed set of tests is rather arbitrary. It would seem desirable to insist that the tests at least reflect the requirements of the particular problem to be solved. For example, it is clear that only the frequency test need be passed if the application is independent of the order in which the numbers appear, as it is in numerical integration. On the other hand it is easy to think of situations in which the order would be extremely important.

Thus a second area that might be worth investigating is one of showing that certain tests reflect the requirements of certain classes of problems. One could study certain canonical problems which might themselves be used for test purposes. Of course it would be particularly gratifying if the performance of particular generators with respect to any such tests could also be predicted theoretically. We must expect that the very best sequences for a particular purpose may be so carefully tailored to that purpose, that they are no longer random. Perhaps some systematic sampling procedures will be needed. One such possibility has already been considered by Richtmyer [102, 103]. See also Halton [47], Hammersley [50], Peck [98], and Richtmyer, Devaney and Metropolis [105].

A third area, which we have studied to some extent, concerns the question of what might be called "local" behavior of our random sequences. To explain, let us first point out that an idealized, completely random sequence can be expected to fail a particular one of the usual statistical tests 5 per cent of the time, as long as we use the 5 per cent level of significance. Thus, if we needed blocks of random numbers for each of a large number of runs, we could expect one block in every twenty to exhibit what we might consider undesirable behavior. Of course what is desirable and what is not desirable must ultimately depend on the problem to be solved.

This possibility of bad "local" behavior even in a sequence with good global behavior, was first mentioned by Kendall and Babington-Smith [61, 62].

We became concerned about the possibility of such bad local behavior occurring even more often than 5 per cent of the time. We conjectured that if this were the case it would be more likely to show up when smaller moduli were being used. The evidence so far is to the effect that with very small moduli, of the order of 2^{12}, there is such a phenomenon associated with some of the multipliers which guarantee maximal periods, but not with the majority. We have so far found no such evidence with moduli of the more usual size (10^{10} and 2^{35}).

The possibility of unsatisfactory local behavior occurring, even in a sequence which as a whole has passed all required tests, suggests that we take some precautions. One such precaution is to have subroutines which not only generate random numbers, but which, when deemed necessary, can be required to accumulate the counts needed for an eventual calculation of the relevant statistics. Perhaps these results could be made available along with the answer, to provide a measure of reliability for the answer.

Some investigations have been made of another class of generators, called "additive". An example of such a generator is obtained if one begins with two integers x_0 and x_1 and then defines the rest of the sequence by means of

$$x_{n+1} \equiv x_n + x_{n-1} \pmod{m}.$$

Results with this simple Fibonacci sequence have not been very satisfactory. A number of variants have been suggested, but they can be much more complicated than the simple one given here. In this case they lose the advantage in speed over our earlier methods. However, it is possible that this class of generators has not received sufficient attention.

Additive generators of various kinds have been considered by Duparc, Lekkerkerker and Peremans [23], Farrington [26], Gilbert [33], Green, Smith and Klem [40], Gross and Johnson [44], Neovius [90], Taussky and Todd [118], van Wijngaarden [130], and Wall [136]. Related mathematical results have been considered by Wall [135], and Mamangakis [74].

Theoretical results regarding periods and other properties of a very general class of sequences, including both multiplicative and additive generators, have recently been given by Zierler [143].

7. HISTORY

The idea of using arithmetic processes for the generation of random numbers is less than fifteen years old. Before describing any further the development that has taken place during this time, we will indicate very briefly what seem to be the main steps leading up to this development.

The general idea of simulation is a very old one. Even the more specific idea of simulation with the help of some particular stochastic process can be traced back several hundred years, to near the beginning of probability theory, to Buffon's needle, and so on.

But the idea of using random sampling to estimate distribution functions, and the beginning of a systematic development of this idea, is apparently due to Student [116] in 1908. Then, and for some time later, random numbers were obtained by drawing cards from a "well-shuffled" deck, by drawing counters from a "well-stirred" urn, or by rolling dice. For relatively recent examples see Hamaker [48], and Walsh [138]. In the last year or two, special icosehedral dice for the generation of decimal digits have been put on the market [128].

The use of cards, counters or dice is a very slow process. Moreover it is extremely difficult to shuffle well, or even to know when you have shuffled well. At Karl Pearson's suggestion, L. H. C. Tippett therefore prepared a list of random digits which he had collected from census reports. Tippett describes his work in a paper [122], published in 1925 in which he states that his digits "were taken at random from census reports"! His table [123] of 41,600 digits first appeared in 1927. In the foreword to this table, Karl Pearson shows how these uniformly distributed digits can be used to give random samples from a distribution which is non-uniform.

A table of 100,000 digits was published in 1939 by Kendall and Babington-Smith [63]. These digits were the first to be produced by a machine. (See also Vickery [131].) Their machine is described in two papers [61, 62] which just preceded the publication of the table. These papers are often referred to, mainly because they contain proposals for the frequency, serial, poker, and gap tests, which we mentioned in section 4. The question of local randomness is also discussed by Kendall and Babington-Smith, and they indicate in their table which blocks do not pass all tests. (There are five such, of 1000 digits each.)

Kendall and Babington-Smith also applied their tests to digits obtained from a telephone directory. They concluded that telephone numbers were an unsatisfactory source of random digits. On the other hand, Kermack and McKendrick had been satisfied with digits they had obtained from telephone numbers. Kendall and Babington-Smith are able to dismiss this apparent discrepancy with the simple remark that Kermack and McKendrick's result "stands in contrast to our results with London telephone numbers, but Kermack and McKendrick are apparently dealing with a five-figure Scottish exchange"!

With Tippett's table as his starting point, Mahalanobis constructed, in 1934, a table of normal deviates [73], but the table contains a number of errors [108]. A corrected version has recently appeared [109]. In 1948 Wold published a table of normal deviates [141], which was based on the table of Kendall and Babington-Smith. Correlated normal deviates have since been published by Fieller [27].

Numerous other tables have been published but we will mention just one more. The most extensive to date was published in 1955 by the RAND Corporation under the title: "A Million Random Digits with 100,000 Normal Deviates" [100]. See also a review by Tompkins [127]. The digits were generated by machinery, as described by Brown [9], and they have been thoroughly tested. They are available on punched cards.

With the introduction of computing machines in the 1940's it became desirable to have more efficient ways of generating random numbers. One suggestion was to build apparatus which could use the "random" signals from some source of electrical noise to produce random numbers within the computer when required. Such apparatus is better known to users of analogue computers. For examples involving digital computers we refer to Golenko and Smiriagin [37], Pawlak [96], Sterzer [115], and von Hoerner [132]. Another machine in current use is ERNIE [7, 121], but this equipment is not part of a computer. It can produce digits at the rate of about fifty per second. But these digits are used solely to determine the numbers in the Premium Savings Bonds lottery, which is operated by the British Post Office.

Although the numbers produced by some of these machines have satisfactorily passed tests for randomness, their use as attachments to general purpose computers is quite unusual. Early concern over maintenance of operation is probably no longer a valid reason, even though a substantial amount of apparatus might be needed to provide numbers rapidly enough for fast machines. It does however seem to be extremely difficult to maintain the randomness itself. Suggestions for removing bias from a sequence of numbers which are not sufficiently random have been given by Horton [52], Horton and Smith [53], Tocher [124], von Neumann [133], Votaw and Rafferty [134], and Walsh [137]. However, to avoid any uncertainty, one might still waste time carrying out tests of the numbers being produced. The cost of the extra equipment does not seem to be justifiable. One final objection arises because, in the course of debugging a program, it is usually advantageous to be able to reproduce calculations exactly.

An alternative to generating numbers as needed is to put a table of random numbers on cards, or on magnetic tape, for use by the computer. The numbers would of course not be stored in the main memory of the computer, and it would be necessary to tie up one input device. Moreover, unless that device is well buffered, the time required will probably be longer than the time needed to generate a number by some arithmetic process.

Thus, since the introduction of computers during the 1940's, there has been a steady interest in the development of efficient and reliable arithmetic generators. Perhaps we should add "at least for most purposes", because we cannot expect an arithmetic generator to replace ERNIE!

The first suggestion for an arithmetic generator was due to von Neumann and Metropolis, in about 1946. This was the "middle-square" method, in which the next number in the sequence is obtained by using the middle digits of the square of the previous number. The method has been discussed by Forsythe [30], Hammer [49], Mauchly [81], Metropolis [82], Taussky and Todd [118], and others. This method is difficult to analyse, and it has not always produced satisfactory results. However runs of about 750,000 numbers were used successfully at Los Alamos for many years [15].

As already mentioned, the invention of multiplicative congruential methods was due to Lehmer [67] in 1949. He first proposed the multiplier $a = 23$, with the modulus $m = 10^8 + 1$, which produced sequences of more than 5 million, 8 decimal digit numbers on ENIAC. Lehmer's method has recently been tested by Liniger [71]. A binary form of Lehmer's method had been tested earlier by Johnson [57]. A variant of the method has been proposed by Page [93].

An apparent advantage of Lehmer's method, over the more usual methods with m a power of 2 or 10, is that the least significant digits do not have short periods.

A radically different generator was recently introduced by von Hoerner [132], and tested by Fisser [28]. It is complicated, and does not seem to offer any advantages over the more usual procedures.

Other alternatives have been based on certain ergodic theorems given by Weyl in 1916 [140]. For example, his theorems guarantee that the fractions $\pi n^2 - [\pi n^2]$, for $n = 1, 2, \cdots$, are uniformly distributed in $(0, 1)$. This suggests that rounded approximations to these fractions might furnish sequences of random numbers. Some work has been published in this area by Bass and Guilloud [2], Franklin [31], and Golenko [35, 36].

The randomness of the digits in the decimal expansions of e and π has been investigated. See Greenwood [43] and the references given by him. However, because of the difficulty of generating such digits, it is not seriously proposed that any method of generation be based on their apparent randomness. A new value of π to 100,000 decimal places has just recently been published [110], but no statistics are reported.

In conclusion it appears that, for Monte Carlo calculations on stored-program computers, the random numbers can be best supplied by an arithmetic generator of either the multiplicative or mixed type. (The only exception would seem to be when one's needs are limited, and when one has available an extra input device which is well buffered.) The mixed methods have a number of theoretical advantages over the multiplicative, but more care is needed in choosing mixed methods which will satisfy the statistical requirements.

Perhaps we can also look forward to a future in which we will be able to provide, on demand, generators to suit specific purposes. The ideal would be to know what statistical properties we required of a particular sequence, and then to design a generator to produce such a sequence. We would use only sequences which were carefully manufactured to suit our purposes. Under such circumstances, how could anyone manage to get along with sequences which were known only to be truly random!

ACKNOWLEDGEMENTS

We wish to express our thanks to the Space and Missiles Division of the Lockheed Aircraft Corporation for enabling us to carry out some of our tests. We are also grateful to Jim Cook of Lockheed for writing some of tbe programs.

John Allard of the Computing Centre at the University of British Columbia has been especially helpful. Besides writing programs, he has made a number of valuable suggestions in connection with this paper.

REFERENCES

1. V. D. Barnett, *The behavior of pseudo-random sequences generated on computers by the multiplicative congruential method*, Math. Comp. 16 (1962), pp. 63–69.
2. J. Bass and J. Guilloud, *Méthode de Monte-Carlo et suites uniformément denses*, Chiffres 1 (1958), pp. 149–156.
3. N. W. Bazley and P. J. Davis, *Accuracy of Monte Carlo methods in computing finite Markov chains*, J. Res. Nat. Bur. Stand. 64B (1960), pp. 211–215.
4. W. F. Bauer, *The Monte Carlo method*, J. Soc. Ind. Appl. Math. 6 (1958), pp. 438–451.
5. Eve Bofinger and V. J. Bofinger, *On a peridoic property of pseudo-random sequences*, J. Assoc. Comp. Mach. 5 (1958), pp. 261–265.
6. Eve Bofinger and V. J. Bofinger, *The gap test for random sequences*, Annals Math. Stat. 32 (1961), pp. 524–534.
7. Eve Bofinger and V. J. Bofinger, *A note on the paper by W. E. Thomson on "ERNIE —a mathematical and statistical analysis"*, J. Roy. Stat. Soc. A124 (1961), pp. 240–243.
8. G. E. P. Box and Mervin E. Muller, *A Note on the generation of random normal deviates*, Annals Math. Stat. 29 (1958), pp. 610–611.
9. George W. Brown, *History of RAND's random digits—summary*, Monte Carlo Method, Nat. Bur. Stand., Appl. Math. Series 12 (1951), pp. 31–32.
10. J. C. Butcher, *A partition test for pseudo-random numbers*, Math. Comp. 15 (1961), pp. 198–199.

11. J. C. Butcher, *Random sampling from the normal distribution*, Comp. J. 3 (1961), pp. 251–253.
12. James W. Butler, *Machine sampling from given probability distributions*, Symposium on Monte Carlo Methods, ed. Herbert A. Meyer, (Wiley, New York, 1956), pp. 249–264.
13. J. M. Cameron, *Monte Carlo experiments on SEAC*, Nat. Bur. Stand., Working Paper SEL-52-5 (Oct. 27, 1951).
14. J. M. Cameron, *Results of some tests of randomness on pseudo-random numbers (preliminary report)*, Annals Math. Stat. 23 (1952), p. 138. Abstract.
15. E. D. Cashwell and C. J. Everett, *A practical manual on the Monte Carlo method for random walk problems* (Pergamon Press, New York, 1959).
16. J. Certaine, *On sequence of pseudo-random numbers of maximal length*, J. Assoc. Comp. Mach. 5 (1958), pp. 353–356.
17. Charles E. Clark, *The utility of statistics of random numbers*, Op. Res. 8 (1960), pp. 185–195.
18. Charles E. Clark and Betty Weber Holz, *Exponentially distributed random numbers* (Johns Hopkins Press, Baltimore, 1960).
19. R. R. Coveyou, *Serial correlation in the generation of pseudo-random numbers*, J. Assoc. Comp. Mach. 7 (1960), pp. 72–74.
20. J. H. Curtiss, *"Monte Carlo" methods for the iteration of linear operators*, J. Math. Phys. 32 (1953), pp. 209–232.
21. P. Davis and P. Rabinowitz, *Some Monte Carlo experiments in computing multiple integrals*, Math. Tables Other Aids Comp. 10 (1956), pp. 1–8.
22. Edward L. Dodd, *Certain tests for randomness applied to data grouped into small sets*, Econometrica 10 (1942), pp. 249–257.
23. H. J. A. Duparc, C. G. Lekkerkerker and W. Peremans, *Reduced sequences of integers and pseudo-random numbers*, Mathematisch Centrum, Amsterdam, Report ZW 1953-002 (1953).
24. A. R. Edmonds, *The generation of pseudo-random numbers on electronic digital computers*, Comp. J. 2 (1960), pp. 181–185.
25. Louis W. Ehrlich, *Monte Carlo solutions of boundary value problems involving the difference analogue of* $\frac{\partial^2 u}{\partial x^2} + \frac{\partial^2 u}{\partial y^2} + \frac{K}{y}\frac{\partial u}{\partial y} = 0$, J. Assoc. Comp. Mach. 6 (1959), pp. 204–218.
26. Carl C. Farrington, Jr., *Generating pseudo-random numbers in the Illiac*, Digital Computer Laboratory Report No. 74, University of Illinois (1956).
27. E. Fieller, *Correlated random normal deviates*, Tracts for Computers, no. 26 (Cambridge, 1955).
28. H. Fisser, *Some tests applied to pseudo-random numbers generated by v. Hoerner's rule*, Numer. Math. 3 (1961), pp. 247–249.
29. G. E. Forsythe, *Generation and testing of 1,217,370 "random" binary digits on the SWAC*, Bull. Am. Math. Soc. 57 (1951), p. 304. Abstract.
30. George E. Forsythe, *Generation and testing of random digits at the National Bureau of Standards, Los Angeles*, Monte Carlo Method, Nat. Bur. Stand., Appl. Math. Series 12 (1951), pp. 34–35.
31. J. N. Franklin, *On the equidistribution of pseudo-random numbers*, Quart. Appl. Math. 16 (1958), pp. 183–188.
32. Robert Gage, *Contents of Tippett's "Random Sampling Numbers"*, J. Am. Stat. Assoc. 38 (1943), pp. 223–227.
33. E. N. Gilbert, *Quasi-random binary sequences*, Bell Telephone Laboratory (Nov. 27, 1953).
34. E. N. Gilbert, *Machine Computation of random numbers*, Bell Telephone Laboratory, MM-56-114-3 (March 12, 1956).

35. D. I. Golenko, *Formation of random numbers with arbitrary law of distribution*, Computational Math., No. 5 (1959), pp. 83–92; in Russian.

36. D. I. Golenko, *Determination of characteristics of some stochastic processes by Monte Carlo methods*, Computational Math., No. 5 (1959), pp. 93–108; in Russian.

37. D. I. Golenko and V. P. Smiriagin, *A source of random numbers which are equidistributed in [0, 1]*, Publications Math. Inst., Hungarian Acad. Sci. 5, Series A, Fasc. 3 (1960), pp. 241–253; in Russian, with English abstract.

38. I. J. Good, *The serial test for sampling numbers and other tests for randomness*, Proc. Camb. Phil. Soc. 49 (1953), pp. 276–284.

39. I. J. Good, *On the serial test for random sequences*, Annals Math. Stat. 28 (1957), pp. 262–264.

40. Bert F. Green, Jr., J. E. Keith Smith and Laura Klem, *Empirical tests of an additive random number generator*, J. Assoc. Comp. Mach. 6 (1959), pp. 527–537.

41. Martin Greenberger, *Notes on a new pseudo-random number generator*, J. Assoc. Comp. Mach. 8 (1961), pp. 163–167.

42. Martin Greenberger, *An a priori determination of serial correlation in computer generated random numbers*, Math. Comp. 15 (1961), pp. 383–389. See also *corrigenda*, Math. Comp. 16 (1962), p. 126.

43. Robert E. Greenwood, *Coupon collector's test for random digits*, Math. Tables Other Aids Comp. 9 (1955), pp. 1–5, 224, 229.

44. O. Gross and S. M. Johnson, *Additive generation of pseudorandom numbers*, RAND Corporation Research Memorandum 2132 (1958).

45. Fred Gruenberger, *Tests of random digits*, Math. Tables Other Aids Comp. 4 (1950), pp. 244–245.

46. Fred Gruenberger and A. M. Mark, *The d^2 test of random digits*, Math. Tables Other Aids Comp. 5 (1951), pp. 109–110.

47. J. H. Halton, *On the efficiency of certain quasi-random sequences of points in evaluating multi-dimensional integrals*, Numer. Math. 2 (1960), pp. 84–90.

48. H. C. Hamaker, *A simple technique for producing random sampling numbers*, Nederl. Akad. Wetensch. Proc. 52 (1949), pp. 145–150.

49. Preston C. Hammer, *The mid-square method of generating digits*, Monte Carlo Method, Nat. Bur. Stand., Appl. Math. Series 12 (1951), p. 33.

50. J. M. Hammersley, *Monte Carlo methods for solving multivariable problems*, Annals N. Y. Acad. Sci. 86 (1960), pp. 844–874.

51. Richard W. Hamming, *Numerical methods for scientists and engineers*, (McGraw-Hill, New York, 1962).

52. H. Burke Horton, *A method for obtaining random numbers*, Annals Math. Stat. 19 (1948), pp. 81–85.

53. H. Burke Horton and R. Tynes Smith III, *A direct method for producing random digits in any number system*, Annals Math. Stat. 20 (1949), pp. 82–90.

54. A. S. Householder (editor, with G. E. Forsythe and H. H. Germond), *Monte Carlo method*, Nat. Bur. Stand., Appl. Math. Series 12 (1951).

55. D. G. N. Hunter, *Note on a test for repeating cycles in a pseudo-random number generator*, Comp. J. 3 (1960), p. 9.

56. International Business Machines Corporation, *Random number generation and testing*, Reference manual C20-8011 (New York, 1959).

57. D. L. Johnson, *Generating and testing pseudo random numbers on the I.B.M. type 701*, Math. Tables Other Aids Comp. 10 (1956), pp. 8–13.

58. M. L. Juncosa, *Random number generation on the BRL high-speed computing machines*, Ballistic Research Laboratories, Report no. 855, (Aberdeen Proving Ground, 1953).

59. Herman Kahn, *Applications of Monte Carlo*, RAND Corporation Research Memorandum 1237 (1956). Also appeared as AECU 3259.

60. HERMAN KAHN, *Use of different Monte Carlo sampling techniques*, Symposium on Monte Carlo methods, ed. Herbert A. Meyer (Wiley, New York, 1956), pp. 146–190.
61. M. G. KENDALL AND B. BABINGTON-SMITH, *Randomness and random sampling numbers*, J. Roy. Stat. Soc. 101 (1938), pp. 147–166.
62. M. G. KENDALL AND B. BABINGTON-SMITH, *Second paper on random sampling numbers*, J. Roy. Stat. Soc., Supplement 6 (1939), pp. 51–61.
63. M. G. KENDALL AND B. BABINGTON-SMITH, *Tables of random sampling numbers*, Tracts for Computers, no. 24 (Cambridge, 1939).
64. W. O. KERMACK AND A. G. MCKENDRICK, *Tests for randomness in a series of numerical observations*, Proc. Roy. Soc. Edinburgh 57 (1937), pp. 228–240.
65. W. O. KERMACK AND A. G. MCKENDRICK, *Some distributions associated with a randomly arranged set of numbers*, Proc. Roy. Soc. Edinburgh 57 (1937), pp. 332–376.
66. HEIDI G. KUEHN, *A 48-bit pseudo-random number generator*, Comm. Assoc. Comp. Mach. 4 (1961), pp. 350–352.
67. D. H. LEHMER, *Mathematical methods in large-scale computing units*, Annals Comp. Laboratory Harvard Univ. 26 (1951), pp. 141–146.
68. D. H. LEHMER, *Combinatorial problems with digital computers*, Proc. Fourth Can. Math. Congress (1957), pp. 160–173.
69. P. H. LESLIE AND J. C. GOWER, *The properties of a stochastic model for two competing species*, Biometrika 45 (1958), pp. 316–330.
70. H. LEVENE AND J. WOLFOWITZ, *The covariance matrix of runs up and down*, Annals Math. Stat. 15 (1944), pp. 58–69.
71. WERNER LINIGER, *On a method by D. H. Lehmer for the generation of pseudo random numbers*, Numer. Math. 3 (1961), pp. 265–270.
72. ERNEST J. LYTLE, JR., *A description of the generation and testing of a set of random normal deviates*, Symposium on Monte Carlo Methods, ed. Herbert A. Meyer (Wiley, New York, 1956), pp. 234–248.
73. P. C. MAHALANOBIS, *Tables of random samples from a normal population*, Sankyhā 1 (1934), pp. 289–328.
74. S. E. MAMANGAKIS, *Remarks on the Fibonacci series modulo m*, Am. Math. Monthly 68, (1961), pp. 648–649.
75. G. MARSAGLIA, *Expressing a random variable in terms of uniform random variables*, Annals Math. Stat. 32 (1961), pp. 894–898.
76. G. MARSAGLIA, *Generating exponential random variables*, Annals Math. Stat. 32 (1961), pp. 899–900.
77. G. MARSAGLIA, *Remark on generating a random variable having a nearly linear density function*, Boeing Scientific Research Laboratories, Mathematical Note no. 242 (Seattle, 1961).
78. G. MARSAGLIA, *Procedures for generating normal random variables, II*, Boeing Scientific Research Laboratories, Mathematical Note no. 243 (Seattle, 1961).
79. ANDREW W. MARSHALL, *The use of multi-stage sampling schemes in Monte Carlo computations*, Symposium on Monte Carlo Methods, ed. Herbert A. Meyer (Wiley, New York, 1956), pp. 123–140.
80. A. DE MATTEIS AND B. FALESCHINI, *Pseudo-random sequences of equal length*, Comitato Nazionale per l'Energia Nucleare, Report no. 88 (Bologna, 1960).
81. J. W. MAUCHLY, *Pseudo-random numbers*, Eckert-Mauchly Computer Corporation Report (1949).
82. N. METROPOLIS, *Phase shifts—middle squares—wave equation*, Symposium on Monte Carlo Methods, ed. Herbert A. Meyer (Wiley, New York, 1956), pp. 29–36.
83. HERBERT A. MEYER, editor, *Symposium on Monte Carlo methods*, (Wiley, New York, 1956).
84. H. A. MEYER, L. S. GEPHART AND N. L. RASMUSSEN, *On the generation and testing of random digits*, Air Res. Dev. Command, WADC Tech. Rep. 54–55 (Wright-Patterson Air Force Base, 1954).

85. JACK MOSHMAN, *The generation of pseudo random numbers on a decimal calculator*, J. Assoc. Comp. Mach. 1 (1954), pp. 88–91.
86. MERVIN E. MULLER, *An inverse method for the generation of random normal deviates on large-scale computers*, Math. Tables Other Aids Comp. 12 (1958), pp. 167–174.
87. MERVIN E. MULLER, *A comparison of methods for generating normal deviates on digital computers*, J. Assoc. Comp. Mach. 6 (1959), pp. 376–383.
88. MERVIN E. MULLER, *A note on a method for generating points uniformly on N-dimensional spheres*, Comm. Assoc. Comp. Mach. 2, no. 4 (1959), pp. 19–20.
89. K. N. NAIR, *On Tippett's random sampling numbers*, Sankhyā 4 (1938), pp. 65–72.
90. GÖSTA NEOVIUS, *Artificial traffic trials using digital computers*, Ericsson Technics 11 (1955), pp. 279–291.
91. GUY H. ORCUTT, MARTIN GREENBERGER, JOHN KORBEL AND ALICE M. RIVLIN, *Microanalysis of socioeconomic systems: a simulation study*, (Harper, New York, 1961).
92. OYSTEIN ORE, *Number theory and its history* (McGraw-Hill, New York, 1948).
93. E. S. PAGE, *The Monte Carlo solution of some integral equations*, Proc. Camb. Phil. Soc. 50 (1954), pp. 414–425.
94. E. S. PAGE, *Pseudo-random elements for computers*, Appl. Stat. 8 (1959), pp. 124–131.
95. G. K. PAKOV, *Generation of a random correlated quantity on a high-speed electronic computer*, Soviet Develop. Infor. Proc. Machine Translat., (U. S. Joint Publ. Res. Service JPRS: 5784, Nov., 1960).
96. Z. PAWLAK, *Flip-flop as generator of random binary digits*, Math. Tables Other Aids Comp. 10 (1956), pp. 28–30.
97. PAUL PEACH, *Bias in pseudo-random numbers*, J. Am. Stat. Assoc. 56 (1961), pp. 610–618.
98. L. G. PECK, *On uniform distribution of algebraic numbers*, Proc. Am. Math. Soc. 4 (1953), pp. 440–443.
99. ANTHONY RALSTON AND HERBERT S. WILF, editors, *Mathematical methods for digital computers* (Wiley, New York, 1960).
100. RAND CORPORATION, *A million random digits with 100,000 normal deviates*, (Free Press, Glencoe, 1955).
101. C. RADHAKRISHNA RAO, *Generation of random permutations of given number of elements using random sampling numbers*, Sankhyā A23 (1961), pp. 305–307.
102. R. D. RICHTMYER, *The evaluation of definite integrals, and a Quasi-Monte-Carlo method based on the properties of algebraic numbers*, Los Alamos Scientific Laboratory, LA-1342 (1951).
103. R. D. RICHTMYER, *A non-random sampling method, based on congruences, for "Monte Carlo" problems*, Institute Math. Sci., NYU, Report NYO-8674 Physics (1958).
104. R. D. RICHTMYER, *Monte Carlo methods*, Nuclear Reactor Theory, Am. Math. Soc., Proc. Symposium Appl. Math. 11 (1961), pp. 190–205.
105. R. D. RICHTMYER, MARJORIE DEVANEY AND N. METROPOLIS, *Continued fraction expansions of algebraic numbers*, Numer. Math. 4 (1962), pp. 68–84.
106. A. C. ROSANDER, *The use of inversions as a tsst of random order*, J. Amer. Stat. Assoc. 37 (1942), pp. 352–358.
107. A. ROTENBERG, *A new pseudo-random number generator*, J. Assoc. Comp. Mach. 7 (1960), pp. 75–77.
108. LORRAINE SCHWARTZ, Review of [73], Math. Tables Other Aids Comp. 8 (1954), p. 228.
109. J. M. SENGUPTA AND NIKHILESH BHATTACHARYA, *Tables of random normal deviates*, Sankhyā 20 (1958), pp. 249–286.
110. DANIEL SHANKS AND JOHN W. WRENCH, JR., *Calculation of π to 100,000 decimals*, Math. Comp. 16 (1962), pp. 76–99.
111. I. M. SOBOL', *Pseudo-random numbers for the machine "Strela"*, Theory Prob. Applications 3 (1958), pp. 192–197.

112. HERBERT SOLOMON, editor, *Studies in item analysis and prediction* (Stanford Univ., Stanford, 1961).
113. J. SPANIER, *A unified approach to Monte Carlo methods and an application to a multigroup calculation of absorption rates*, This Review, to appear.
114. GORDON SPENSER, *Random numbers and their generation*, Computers and Automation 4, no. 3 (1955), pp. 10–11 and 23.
115. FRED STERZER, *Random number generator using subharmonic oscillators*, Rev. Sci. Insts. 30 (1959), pp. 241–243.
116. STUDENT, *The probable error of a mean*, Biometrika 6 (1908), pp. 1–25.
117. FRIEDA S. SWED AND C. EISENHART, *Tables for testing randomness of grouping in a sequence of alternatives*, Annals Math. Stat. 14 (1943), pp. 66–87.
118. OLGA TAUSSKY AND JOHN TODD, *Generation and testing of pseudo-random numbers*, Symposium on Monte Carlo Methods, ed. Herbert A. Meyer (Wiley, New York, 1956), pp. 15–28.
119 D. TEICHROEW, *Distribution sampling with high speed computers*, Diss., Univ. of North Carolina (1953).
120. W. E. THOMSON, *A modified congruence method of generating pseudo-random numbers*, Comp. J. 1 (1958), pp. 83, 86.
121. W. E. THOMSON, *ERNIE—A* mathematical and statistical analysis, J. Roy. Stat. Soc. A122 (1959), pp. 301–324; discussion pp. 324–333.
122. L. H. C. TIPPETT, *On the extreme individuals and the range of samples taken from a normal population*, Biometrika 17 (1925), pp. 364–387.
123. L. H. C. TIPPETT, *Random sampling numbers*, Tracts for Computers, no. 15 (Cambridge, 1927).
124. K. D. TOCHER, *The application of automatic computers to sampling experiments*, J. Roy. Stat. Soc. B16 (1954), pp. 39–61; discussion pp. 61–75.
125. JOHN TODD, *Experiments in the solution of differential equations by Monte Carlo methods*, J. Wash. Acad. Sci. 44 (1954), pp. 377–381.
126. JOHN TODD, editor, *Survey of numerical analysis* (McGraw-Hill, New York, 1962).
127. C. B. TOMPKINS, Review of [100], Math. Tables Other Aids Comp. 10 (1956), pp. 39–43.
128. C. B. TOMPKINS, *Review of "Japanese Standards Association, random number generating icosahedral dice"*, Math. Comp. 15 (1961), pp. 94–95.
129. C. B. TOMPKINS, *Machine attacks on problems whose variables are permutations*, Numerical Analysis, Amer. Math. Soc., Proc. Symposium Appl. Math. 6 (McGraw-Hill, New York, 1956), pp. 195–212.
130. A. VAN WIJNGAARDEN, *Mathematics and computing*, Automatic Digital Computation, Proc. Symposium, National Physical Laboratory (H.M.S.O., London, 1954), pp. 125–129.
131. C. W. VICKERY, *On drawing a random sample from a set of punched cards*, J. Roy. Stat. Soc., Supplement 6 (1939), pp. 62–66.
132. SEBASTIAN VON HOERNER, *Herstellung von Zufallszahlen auf Rechenautomaten*, Zeit. Angew. Math. Physik 8 (1957), pp. 26–52.
133. JOHN VON NEUMANN, *Various techniques used in connection with random digits*, Monte Carlo Method, Nat. Bur. Stand., Appl. Math. Series 12 (1951), pp. 36–38.
134. D. F. VOTAW, JR. AND J. A. RAFFERTY, *High Speed sampling*, Math. Tables Other Aids Comp. 5 (1951), pp. 1–8.
135. D. D. WALL, *Fibonacci series modulo m*, Amer. Math. Monthly 67 (1960), pp. 525–532.
136. DONALD D. WALL, *A random number test for large samples*, Proc. First IBM Conf. Stat. (Poughkeepsie, 1960), pp. 7–11.
137. JOHN E. WALSH, *Concerning compound randomization in the binary system*, Annals Math. Stat. 20 (1949), pp. 580–589.
138. JOHN E. WALSH, *An experimental method for obtaining random digits and permutations*, Sānkhyā 17 (1957), pp. 355–360.

139. JAMES G. WENDEL, *Lectures on Monte Carlo,* Univ. of Mich., Summer Session Courses on Numerical Analysis (1961).
140. H. WEYL, *Über die Gleichverteilung von Zahlen mod. Eins,* Math. Annalen 77 (1916), pp. 313–352.
141. HERMAN WOLD, *Random normal deviates,* Tracts for Computers, no. 25 (Cambridge, 1948).
142. G. UDNY YULE, *A test of Tippett's random sampling numbers,* J. Roy. Stat. Soc. 101 (1938), pp. 167–172.
143. NEAL ZIERLER, *Linear recurring sequences,* J. Soc. Ind. Appl. Math. 7 (1959), pp. 31–48.

SUPPLEMENTARY REFERENCES

Added in Proof

Several additional references have recently come to our attention.

Franklin [3′] has given a very thorough theoretical study of the statistical properties of several sequences including the Weyl sequence, and the mixed congruential sequence (which he calls the multiply sequence). Although he does not consider the restrictions imposed by the finite word-length of a computer, his results are certainly suggestive of what might be expected in practice.

A text on Monte Carlo methods has appeared in Russian [1′]. Its first chapter is entitled "Construction of a set of random numbers on electronic digital computers".

Isida and Ikeda [4′] describe apparatus for the generation of random digits. Pathria [5′] reports on the statistics of the first 10,000 digits in π. Clark [2′] reports errors in a paper by Muller [86].

1′. N. P. BUSLENKO AND JU. A. SREIDER, *The Monte-Carlo method and how it is carried out on digital computers,* (Gosudarstv. Izdat. Fiz-Mat. Lit., Moscow, 1961) (Russian).
2′. G. MILLER CLARK, Corrections to [86], Math. Comp. 16 (1962), p. 261.
3′. JOEL N. FRANKLIN, *Deterministic simulation of random processes,* Computing Center, California Institute of Technology, Technical Report No. 118 (1962).
4′. MASATUGU ISIDA AND HIROJI IKEDA, *Random number generator,* Ann. Inst. Statist. Math. (Tokyo) 8 (1956), pp. 119–126.
5′. R. K. PATHRIA, *A statistical study of randomness among the first 10,000 digits of π,* Math. Comp. 16 (1962), pp. 188–197.