The Behavior of Pseudo-Random Sequences Generated on Computers by the Multiplicative Congruential Method

By V. D. Barnett

1. Introduction. The use of pseudo-random elements in Monte Carlo work is essential when the scale of this work is such that the calculations involved are too extensive for hand calculating machines and it is necessary to employ an electronic computer. Although the ability of modern digital computers to perform simple binary operations at very high speed makes their use in this work particularly relevant, the limited extent of the computer memory, the relatively slow input speeds and speeds of access to the memory, and the very large number of random elements required (often of the order of 10^6) combine to make it unfeasible to prepare the elements beforehand in the required form for input to the computer (e.g., on tape or cards), and we must resort to some means of generation of the random elements within the computer.

Mechanical means of generation on peripheral equipment, e.g., by radioactive decay, thermal noise in electronic valves, etc., are undesirable because of the irreproducibility of the numbers obtained, which enables no check to be kept on their quality. It is therefore natural to employ some deterministic method of generation of the random elements by recurrence relationships. One such technique which has attracted much attention is the multiplicative congruential method (see for example [1], [2] and [3]) which proceeds as follows:

Choose ρ, x at random as the starting values.

Successive random elements are then obtained by the recurrence relationship

$$x_{r+1} \equiv x \cdot x_r \pmod{M} \tag{1}$$

with $x_0 = \rho$: that is, x_{r+1} is of the form $\rho x^r \pmod{M}$.

Using this method to generate pseudo-random sequences, one must place certain restrictions on x and ρ to ensure that the process does not degenerate to zero and that the maximum possible cycle of distinct elements is obtained. We shall see that only two restrictions must be placed on x and ρ to produce the maximum cycle and that it is also possible to describe fully the behavior of the system for x and ρ not satisfying these restrictions.

Because of the binary base of most digital computers, it is convenient to choose M of the form 2^k. Reduction, modulo M, is then simply a shift of the product ρx^r to retain the least significant k binary digits. If the computer, in common with many modern computers, has a facility for low multiplication, i.e., multiplication which retains only the least significant half of the set of binary digits comprising the product, and the numbers are stored as k_0 digits, it is a further advantage to choose

$$M = 2^{k_0},$$

Received May 8, 1961.

and this enables the successive random elements to be obtained by just one operation.

The length of the cycle of iterates and the conditions under which the maximum cycle is obtained must obviously depend on ρ, x, and $M = 2^k$, and although this system (for $M = 2^k$) is discussed in the literature [1], [4], [5], there appears to be some confusion as to the behavior of the system for given ρ, x, and M.

It has often been assumed desirable to choose x of the form

$$x = 5^{2k+1}$$

$$x = 7^{4k+1}$$

$$x = 13^{13} \text{ etc.}$$

to ensure the maximum cycle; see [3]. For instance, Taussky and Todd [1] state that for the system

$$\rho \equiv 1 \pmod 5$$

$$x = 5^{17}$$

$$M = 2^{42}$$

they obtain a cycle of length 2^{40}. We see immediately in this case that the cycle cannot be of length 2^{40}. As they demonstrate in the same paper, for an x in this form (i.e., $\equiv 5 \pmod 8$) the periods of successive digits from the least significant digit are as follows: 1, 1, 2, 4, 8, 16, $\cdots$, the least significant digit being always 1, the next always 0, the next alternately 0 or 1 the next 0, 0, 1, 1 and so on.

Now, if we choose ρ to be of the form 1 (mod 5), say $\rho = 256 = 2^8$, then the effect of multiplying the successive powers of x by 2^8 and reducing the product modulo 2^{42} is to shift each digit to a position 8 places more significant and to fill in the 8 least significant places with zeros. Because of the strict increase by factors of 2 in the period of the digits as they become more significant, this must result in a reduction of the length of the maximum cycle by the factor 2^8. (No formal proof of this maximum appears to have been given previously.)

This example should suffice to illustrate the importance of obtaining a set of necessary and sufficient conditions on ρ and x for the maximum cycle-length to be achieved, and also of giving a description of the behavior of the system when these conditions are not satisfied.

The only attempts to define formally the restrictions necessary on ρ and x are those of Leslie and Gower [4] and Certaine [5].

Leslie and Gower state that a maximum period of 2^{k-2} distinct random elements is obtained subject to:

(1) Choosing ρ and x' at random;

(2) Replacing x' by x the closest number to x' such that $x \equiv 5 \pmod 8$;

(3) Forming successively the numbers $\rho x^r \pmod{2^k}$, $r = 1, 2, \cdots$.

The random elements are then all 2^{k-2} numbers (mod 2^k) whose least significant binary digits are 10. This result is attributed to a theorem by Euler.

On examination we find that condition (2) on x is more restrictive than is necessary; and, as we have already seen, it is essential that some restriction be placed on ρ.

A discussion of the form of x necessary to ensure a cycle of maximum length and of the length of this maximum cycle has been given by Certaine [5] for general M, but his conclusions on the form of x for the particular case

$$M = 2^k$$

would again appear to be unnecessarily restrictive.

Furthermore, no attempt has been made to describe in what way the system is affected by a choice of x and ρ which do not satisfy the conditions required for the maximum cycle.

The system of numbers obtained from equation (1) for $M = 2^k$ is fully described in the following section, the proofs of the results being given in Section 3.

2. Formal Description of System of Numbers Generated by $x_{r+1} = x \cdot x_r \pmod{2^k}$; $\rho = x_0$. Under favorable conditions on x and ρ we obtain a maximum cycle of 2^{k-2} elements, all of which are distinct. The conditions on x and ρ to achieve this maximum cycle are:

I: $x \equiv \pm 5 \pmod 8$, i.e.

$x \equiv 5 \pmod 8$ or $x \equiv 3 \pmod 8$

II: $\rho \equiv 1 \pmod 2$, i.e.

ρ must be odd.

I and II are necessary and sufficient for the maximum cycle to be obtained.

Relaxation of these conditions affects the length of the cycle, and in some cases causes the process to degenerate to zero.

2.1. Relaxation of Condition II. If ρ is even and condition I is satisfied, the maximum cycle of 2^{k-2} distinct iterates is reduced in length by a factor 2^j where this is the highest power of two by which ρ is divisible, i.e., if $\rho \equiv 2^j \pmod{2^{j+1}}$ the cycle is of length 2^{k-j-2}.

We have already seen an illustration of this effect in the discussion of the system described by Taussky and Todd [1].

2.2. Relaxation of Condition I.

(a) If x is even, the maximum number of distinct iterates is k, generated by $x \equiv 2 \pmod 4$. In general, if $x \equiv 2^j \pmod{2^{j+1}}$ the number of distinct iterates is $\left[\frac{k}{j}\right]$ (where $[z]$ signifies the least integer greater than, or equal to, z). In all cases for x even the process degenerates to zero on the $\left[\frac{k}{j}\right]$th element produced. If ρ is even, say $\rho \equiv 2^l \bmod 2^{l+1}$, the process degenerates to zero on the $\left[\frac{k-l}{j}\right]$th element produced.

(b) If x is odd, the maximum cycle is generated, consisting of 2^{k-2} distinct iterates, if and only if

$$x \equiv 3 \text{ or } 5 \pmod 8.$$

For any other odd values of x the length of the cycle is decreased as follows:

$$\text{If } x \equiv 7 \text{ or } 9 \pmod{16}, \text{ length of cycle is } 2^{k-3};$$

$$\text{If } x \equiv 15 \text{ or } 17 \pmod{32}, \text{ length of cycle is } 2^{k-4}, \text{ etc.}$$

We may completely specify all odd integers in this way, with the general result that if $x \equiv 2^j \pm 1 \pmod{2^{j+1}}$ the length of the cycle obtained is $2^{k-j}; j \geqq 2$; all iterates being distinct.

We may summarize these results as follows.

If $k = 2, 3$ the maximum number of distinct elements is k, generated by $x \equiv 2 \pmod 4$, $\rho \equiv 1 \pmod 2$, and the process degenerates to zero.

If $k > 3$ the maximum cycle is of 2^{k-2} distinct elements and is generated by $x \equiv 3$ or $5 \pmod 8$, again for $\rho \equiv 1 \pmod 2$.

Small values of k are, of course, of little practical interest in the generation of pseudo-random elements.

Relaxation of the conditions I and II simultaneously has the effect of combining the results of paragraphs (a) and (b). For example,

$$\left.\begin{aligned} \rho &\equiv 2 \pmod 4 \\ x &\equiv 7 \pmod{16} \end{aligned}\right\}$$

will produce a cycle of 2^{k-4} distinct elements, or, again,

$$\left.\begin{aligned} \rho &\equiv 2 \pmod 4 \\ x &\equiv 2 \pmod 4 \end{aligned}\right\}$$

will produce $\left(\left[\frac{k-1}{2}\right]\right)$ distinct elements, the process degenerating to zero.

3. Proof of Results of Section 2. Let us first consider condition I. For general x we have two possibilities:

$$x \text{ even: i.e., } x = 2m$$

$$x \text{ odd: } x = 2m + 1$$

3.1. x even. $M = 2^k$

Let $N(x) = [k/I(x)]$ where $I(x)$ is the index of the greatest power of 2 which divides x. Then

$$I(x^{N(x)}) \geqq k \text{ (since } I(x^m) = mI(x) \not\equiv 0).$$

Hence $x^{N(x)} \equiv 0 \pmod{2^k}$ and number of distinct iterates cannot be greater than $N(x)$, for at this stage the process degenerates to zero.

Further, by the definition of $N(x)$, the process cannot terminate earlier.

Also, if $0 \leqq m, n \leqq N(x) \Rightarrow a^m \equiv a^n \pmod{2^k}$, then

$$a^{m-n} \equiv 1 \pmod{2^k}$$

and hence

$$m - n = 0.$$

Therefore, the congruence classes of the $N(x) + 1$ powers of x: $1, x, x^2, \cdots, x^{N(x)}$, are distinct and we must obtain $N(x)$ distinct iterates up to degeneration of the process (x^0 not being obtained). $N(x)$ will be a maximum for $N(x) = k$, i.e., $I(x) = 1$. So $x \equiv 2 \pmod 4$ generates k distinct elements, and in general $x \equiv 2^j \pmod{2^{j+1}}$ generates $\left[\frac{k}{j}\right]$.

3.2. x odd. $M = 2^k; x = 2m + 1.$

LEMMA. $Z - I(Z) \geqq 5$ *for* $Z \geqq 5$

Proof. If $2^i \leqq Z < 2^{i+1}$ then $I(Z) \leqq i$. Thus $Z - I(Z) \geqq 2^i - i$ which is monotone increasing in i and so $\geqq 5$ for $i \geqq 3$, i.e., for $Z \geqq 8$. Also if $Z = 5, 6, 7$ then $I(Z) = 0, 1, 0$ respectively. Hence $Z - I(Z) \geqq 5$, all $Z \geqq 5$ as required.

Now if $x = 2m + 1$, the 2^{k-1} congruence classes of x in the range $(0, 2^k)$ form a multiplicative group, the order $n(x)$ of the congruence class of x being the least integer such that

$$x^{n(x)} \equiv 1 \pmod{2^k},$$

hence, $n(x)$ divides 2^{k-1} [6].

Furthermore, the congruence classes of $x, x^2, \cdots, x^{n(x)}$ include all powers of x and are distinct, for if

$$x^m \equiv x^n \pmod{2^k} \qquad m > n, \quad \text{then}$$
$$x^{m-n} \equiv 1 \pmod{2^k},$$

and $m - n$ must be greater than $n(x)$.

So we see that the cycles generated by odd integers have length of a power of 2, the maximum cycle being given by the odd integer of greatest order in the group, and we must find the conditions necessary on x for it to have this greatest order. That the process must cycle is obvious, for if

$$x^j \equiv 0 \pmod{2^k}, \quad \text{then}$$
$$x \equiv 0 \pmod{2^k} \quad \text{since} \quad x \not\equiv 2^k$$

i. e., x is even, which is not true.

Now, $n(x)$ is determined by

$$(1 + 2m)^{2^l} \not\equiv 1 \pmod{2^k}$$

but $(1 + 2m)^{2^{l+1}} \equiv 1 \pmod{2^k}$, where $l = I(n(x)) - 1$.

Consider $(1 + 2m)^{2^l} \pmod{2^{l+p}}$ for suitable p.

If $p = 3$, then

$$I\left\{(2m)^r \binom{2^l}{r}\right\} \geqq r - I(r) + l$$
$$\geqq l + 5 \quad \text{for} \quad r \geqq 5.$$

Thus

$$(1 + 2m)^{2^l} \equiv \left\{\sum_0^4 (2m)^r \binom{2^l}{r}\right\} \pmod{2^{l+3}}, \tag{2}$$

and setting $\phi = (1 + 2m)^{2^l} - 1$, we have

$$\phi \equiv \left[2^{l+1}m + 2^{l+1}(2^l - 1)m^2 + \frac{2^{l+3}}{3}(2^l - 1)(2^{l-1} - 1)m^3 + \frac{2^{l+2}}{3}(2^l - 1)(2^{l-1} - 1)(2^l - 3)m^4\right] \pmod{2^{l+3}}.$$

Hence, if $l \geqq 2$

$$\begin{aligned}\phi &\equiv 2^{l+1}[m - m^2 - 2m^4] \pmod{2^{l+3}} \\ &\equiv 2^{l+1}[m(m+1) - 2m^2(m^2+1)] \pmod{2^{l+3}} \\ &\equiv 2^{l+1}m(m+1) \pmod{2^{l+3}}\end{aligned}$$

(for if m odd or even $2m^2(m^2 + 1) \equiv 0 \pmod 4$).

We must now distinguish between

$$\text{(i)}\ m \equiv 0, -1 \pmod 4$$

$$\text{(ii)}\ m \equiv 1, 2 \pmod 4.$$

(i) $(1 + 2m)^{2^l} - 1 \equiv 0 \pmod{2^{l+3}}$ hence, if $l + 3 = k$, $x^{M/8} \equiv 1 \pmod M$) so that $n(x)$ divides $M/8$.

(ii) $(1 + 2m)^{2^l} - 1 \equiv 0 \pmod{2^{l+2}}$ (for $m(m + 1) \equiv 2 \pmod 4$ but $(1 + 2m)^{2^l} - 1 \not\equiv 0 \pmod{2^{l+3}}$. Hence, taking $k = l + 2$; $k = l + 3$, we have $x^{M/4} \equiv 1$, $x^{M/8} \not\equiv 1$, (mod M), so that the maximum value of $n(x)$ is $M/4$, and it assumes this value for all $x = 1 + 2m$, where $m \equiv 1, 2 \pmod 4$, i.e.,

$$x \equiv 3 \pmod 8, \quad \text{or}$$

$$x \equiv 5 \pmod 8$$

and only these values.

Taking $p = 4$, we again find that

$$\phi \equiv m(m + 1)2^{l+1} \pmod{2^{l+4}} \qquad (l \geqq 3)$$

and we can immediately determine for what values of x we obtain the next largest cycle.

For this we want

$$m(m + 1) \equiv 0 \pmod 4, \quad \text{and}$$

$$m(m + 1) \not\equiv 0 \pmod 8, \quad \text{i.e.}$$

$$m \equiv 3, 4 \pmod 8, \quad \text{giving}$$

$$x \equiv 7, 9 \pmod{16}.$$

Similarly, we may extend this result by suitable choice of p to show that in general we obtain a maximum cycle of 2^{k-j} distinct elements for

$$x \equiv 2^j \pm 1 \pmod{2^{j+1}}.$$

This completely specifies the system for all odd x, for any odd value of x can be expressed in the form

$$x \equiv 2^j \pm 1 \pmod{2^{j+1}}, \qquad j = 2, 3, \cdots$$

($x = 1$ is, of course, trivial).

We now consider the effect of different values of ρ on these results. Any value of x which is of the form $x \equiv 2^j \pm 1 \pmod{2^{j+1}}$; $j \geqq 2$, i.e., any odd value of x, produces a cycle of 2^{k-j} distinct elements having the following characteristics:

(a) The least significant digit is 1;

(b) The least significant $j + 2$ digits are of total order 4;

(c) The order of the $(j + 3)$th digit is 2, the order of the $(j + 4)$th digit is 4, etc.; that is, the order of the successive digits beyond the $(j + 2)$th have orders which increase by the factor 2 as they become increasingly more significant.

Therefore, it is apparent by inspection that the effect of multiplication of the elements by any odd value of ρ will be to leave these characteristics invariant and to unalter the length of the cycle of elements obtained.

Furthermore, if ρ is even, say $\rho \equiv 2^r \pmod{2^{r+1}}$, the r least significant digits must become zero and the above characteristics will then be true for the remaining $k - r$ digits, i.e., multiplication by an even-valued ρ has the effect of shifting the digits to a position r places more significant, performing a permutation of the digits remaining after such a shift, which does not affect their order, and substituting zeros for the least significant r digits. This must result in a reduction in the length of the cycle of elements by the factor 2^r.

These remarks are easily verified if we consider the effect of multiplication by ρ of the equation (2) for suitable choice of p for the form of x to be studied.

If, however, x is even, say $x \equiv 2^j \pmod{2^{j+1}}$, the successive powers of x have j, $2j$, $\cdots$ zeros as their least significant j, $2j$, $\cdots$ digits, and multiplication by any odd-valued ρ cannot affect the number of distinct iterates before degeneration, for it must ensure that in the successive iterates the $(j + 1)$th, $(2j + 1)$th$\cdots$ digits are non-zero.

When ρ is even, say $\rho \equiv 2^r \pmod{2^{r+1}}$, multiplication by ρ will introduce r further zeros in place of the r least significant non-zero digits and will therefore reduce the number of iterates to $\left[\frac{k-r}{j}\right]$.

4. Acknowledgment. I am indebted to Dr. M. C. Barratt of the Department of Mathematics in the University of Manchester for the substance of the proof of the behavior of the system for odd values of x.

Statistical Laboratory
University of Manchester
England

1. O. Taussky & J. Todd, "The generation and testing of pseudo-random numbers," *Symposium on Monte Carlo Methods*, John Wiley & Sons, Inc., New York, 1954.
2. K. D. Tocher, "The application of automatic computers to sampling experiments," *J. Roy. Statist. Soc.* Ser. B, v. 16, 1954.
3. E. S. Page, "Pseudo-random elements for computers," *Appl. Statist.*, v. 8, 1959.
4. P. H. Leslie & J. C. Gower, "The properties of a stochastic model for two competing species," *Biometrika*, v. 45, 1958.
5. J. Certaine, "On sequences of pseudo-random numbers of maximal length," *J. Assoc. Comp. Mach.*, v. 5, 1958.
6. W. Ledermann, *The Theory of Finite Groups*, Oliver & Boyd, London, 1949.