RANDOM NUMBERS FALL MAINLY IN THE PLANES

By George Marsaglia

MATHEMATICS RESEARCH LABORATORY, BOEING SCIENTIFIC RESEARCH LABORATORIES, SEATTLE, WASHINGTON

Communicated by G. S. Schairer, June 24, 1968

Virtually all the world's computer centers use an arithmetic procedure for generating random numbers. The most common of these is the multiplicative congruential generator first suggested by D. H. Lehmer. In this method, one merely multiplies the current random integer I by a constant multiplier K and keeps the remainder after overflow:

$$\text{new } I = K \times \text{old } I \quad \text{modulo } M.$$

The apparently haphazard way in which successive multiplications by a large integer K produce remainders after overflow makes the resulting numbers work surprisingly well for many Monte Carlo problems. Scores of papers have reported favorably on cycle length and statistical properties of such generators.

The purpose of this note is to point out that all multiplicative congruential random number generators have a defect—a defect that makes them unsuitable for many Monte Carlo problems and that cannot be removed by adjusting the starting value, multiplier, or modulus. The problem lies in the "crystalline" nature of multiplicative generators—if n-tuples $(u_1,u_2,\ldots,u_n)$, $(u_2,u_3,\ldots,u_{n+1}),\ldots$ of uniform variates produced by the generator are viewed as points in the unit cube of n dimensions, then *all* the points will be found to lie in a relatively small number of parallel hyperplanes. Furthermore, there are many systems of parallel hyperplanes which contain all of the points; the points are about as randomly spaced in the unit n-cube as the atoms in a perfect crystal at absolute zero.

One can readily think of Monte Carlo problems where such regularity in "random" points in n-space would be unsatisfactory; more disturbing is the possibility that for the past 20 years such regularity might have produced bad, but unrecognized, results in Monte Carlo studies which have used multiplicative generators.

Some Notation.—For any modulus m and multiplier k, let

$$r_1,r_2,r_3,\ldots \quad 0 < r_i < m$$

be a sequence of residues of m generated by the recurrence relation

$$r_{i+1} \equiv kr_i \text{ modulo } m,$$

and let $u_1,u_2,u_3,\ldots$ be that sequence viewed as fractions of m:

$$u_1 = r_1/m,\ u_2 = r_2/m,\ u_3 = r_3/m,\ldots.$$

Let $\pi_i = (u_1,\ldots,u_n)$, $\pi_2 = (u_2,\ldots,u_{n+1})$, $\pi_3 = (u_3,\ldots,u_{n+2})$, ... be points of the unit n-cube formed from n successive u's.

THEOREM 1. *If $c_1,c_2,\ldots,c_n$ is any choice of integers such that*

$$c_1 + c_2k + c_3k^2 + \ldots + c_nk^{n-1} \equiv 0 \text{ modulo } m,$$

then all of the points $\pi_1,\pi_2,\ldots$ will lie in the set of parallel hyperplanes defined by the equations

$$c_1x_1 + c_2x_2 + \ldots + c_nx_n = 0, \pm 1, \pm 2, \ldots .$$

There are at most

$$|c_1| + |c_2| + \ldots + |c_n|$$

of these hyperplanes which intersect the unit n-cube, and there is always a choice of $c_1,c_2,\ldots,c_n$ such that all of the points fall in fewer than $(n!m)^{1/n}$ hyperplanes.

Here is a table of $(n!m)^{1/n}$ for the most common values of m, powers of 2:

Upper Bound for the Number of Planes Containing All n-tuples

	$n = 3$	$n = 4$	$n = 5$	$n = 6$	$n = 7$	$n = 8$	$n = 9$	$n = 10$
$m = 2^{16}$	73	35	23	19	16	15	14	13
$m = 2^{24}$	465	141	72	47	36	30	26	23
$m = 2^{32}$	2,953	566	220	120	80	60	48	41
$m = 2^{35}$	5,907	952	333	170	108	78	61	51
$m = 2^{36}$	7,442	1,133	383	191	119	85	66	54
$m = 2^{48}$	119,086	9,065	2,021	766	391	240	167	126

For example, in a binary computer with 32-bit words, $m = 2^{32}$, fewer than 41 hyperplanes will contain all 10-tuples, fewer than 566 hyperplanes will contain all 4-tuples, and fewer than 2,953 planes will contain all 3-tuples. (The generator $r_{i+1} \equiv kr_i \bmod 2^{32}$ will produce 357,913,941 independent points in the unit 3-cube, and theoretically the smallest number of planes containing all these points is about 10^8, in contrast to the bound of 2,953.)

The theorem can be proved in four steps:

Step 1: If

$$c_1 + c_2k + c_3k^2 + \ldots + c_nk^{n-1} \equiv 0 \text{ modulo } m,$$

then

$$c_1u_i + c_2u_{i+1} + \ldots + c_nu_{i+n-1}$$

is an integer for every i, and thus

Step 2: The point $\pi_i = (u_i, u_{i+1},\ldots,u_{i+n-1})$ must lie in one of the hyperplanes

$$c_1x_1 + c_2x_2 + \ldots + c_nx_n = 0, \pm 1, \pm 2, \pm 3, \ldots .$$

Step 3: The number of hyperplanes of the above type which intersect the unit n-cube, $0 < x_1 < 1, \ldots, 0 < x_n < 1$, is at most

$$|c_1| + |c_2| + \ldots + |c_n|,$$

and

Step 4: For every multiplier k and modulus m there is a set of integers $c_1,\ldots, c_n$ (not all zero) such that

$$c_1 + c_2k + c_3k^2 + \ldots + c_nk^{n-1} \equiv 0 \text{ modulo } m$$

and

$$|c_1| + |c_2| + \ldots + |c_n| \leq (n!m)^{1/n}.$$

To prove Step 1, note that by using the greatest integer notation [ ], the sequence $r_1,r_2,\ldots$ can be put in the form

$$r_1,\ kr_1 - m[kr_1/m],\ k^2r_1 - m[k^2r_1/m],\ k^3r_1 - m[k^3r_1/m],\ldots$$

and thus the sequence $u_1,u_2,\ldots$ may be written

$$\frac{r_1}{m} - \left[\frac{r_1}{m}\right], \frac{kr_1}{m} - \left[\frac{kr_1}{m}\right], \frac{k^2r_1}{m} - \left[\frac{k^2r_1}{m}\right], \frac{k^3r_1}{m} - \left[\frac{k^3r_1}{m}\right], \ldots.$$

Clearly, if $c_1 + c_2k + \ldots + c_nk^{n-1}$ is a multiple of m, then $c_1u_i + \ldots + c_nu_{i+n-1}$ will be an integer.

Step 2 follows immediately from Step 1, and Step 3 is easily verified.

Now, for Step 4 we want to prove that there are integers $c_1,c_2,\ldots,c_n$ not all zero such that

$$c_1 + c_2k + c_3k^2 + \ldots + c_nk^{n-1} \equiv 0 \text{ modulo } m \tag{1}$$

and

$$|c_1| + |c_2| + \ldots + |c_n| \leq (n!m)^{1/n}.$$

To do this we transform the problem so that it becomes a standard one in the geometry of numbers: every solution to (1) can be expressed (uniquely) by the relation

$$(c_1,\ldots,c_n) = (t_1,\ldots,t_n)\begin{pmatrix} m & 0 & 0 & 0 & \ldots & 0 & 0 \\ -k & 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & -k & 1 & 0 & \ldots & 0 & 0 \\ \vdots & & & & & & \\ 0 & 0 & 0 & 0 & \ldots & -k & 1 \end{pmatrix},$$

where the t's are integers. Thus the problem is to show that there are integers $t_1,\ldots t_n$ not all zero such that

$$|mt_1 - kt_2| + |t_2 - kt_3| + \ldots + |t_{n-1} - kt_n| + |t_n| \leq (n!m)^{1/n}.$$

This follows from a general theorem on linear forms by Minkowski, using the basic result that a symmetric, convex set of volume 2^n in n-space must contain a point (other than the origin) with integral coordinates. Elegant, elementary proofs are now available; see, e.g., Hardy and Wright,[2] pages 394–396 and 413, or Cassels,[1] pages 150–153.

Step 4 together with the Steps 1–3 complete the proof of Theorem 1—every multiplicative random number generator produces n-tuples of uniform variates which lie in at most $(n!m)^{1/n}$ parallel hyperplanes. Furthermore, any choice of $c_1,\ldots,c_n$ which satisfies congruence (1) will provide a set of at most $|c_1| + \ldots + |c_n|$ parallel hyperplanes which contain all of the n-tuples produced by the generator. Similar results can be established for congruential generators of the type $r_{i+1} \equiv kr_i + c \bmod m$.

[1] Cassels, J. W. S., *An Introduction to Diophantine Approximation* (London: Cambridge University Press, 1965).

[2] Hardy, G. H., and E. M. Wright, *An Introduction to the Theory of Numbers* (Oxford University Press, 1960), 4th ed.