MATHEMATICS OF COMPUTATION
VOLUME 54, NUMBER 189
JANUARY 1990, PAGES 331-344

MULTIPLICATIVE CONGRUENTIAL RANDOM NUMBER GENERATORS WITH MODULUS 2^{β}: AN EXHAUSTIVE ANALYSIS FOR $\beta = 32$ AND A PARTIAL ANALYSIS FOR $\beta = 48$

GEORGE S. FISHMAN

ABSTRACT. This paper presents the results of a search to find optimal maximal period multipliers for multiplicative congruential random number generators with moduli 2^{32} and 2^{48}. Here a multiplier is said to be optimal if the distance between adjacent parallel hyperplanes on which k-tuples lie does not exceed the minimal achievable distance by more than 25 percent for $k = 2, \ldots, 6$. This criterion is considerably more stringent than prevailing standards of acceptability and leads to a total of only 132 multipliers out of the more than 536 million candidate multipliers that exist for modulus 2^{32} and to only 42 multipliers in a sample of about 67.1 million tested among the more than 351×10^{11} candidate multipliers for modulus 2^{48}.

Section 1 reviews the basic properties of multiplicative congruential generators and §2 describes *worst case* performance measures. These include the maximal distance between adjacent parallel hyperplanes, the minimal number of parallel hyperplanes, the minimal distance between k-tuples and the discrepancy. For modulus 2^{32}, §3 presents the ten best multipliers and compares their performances with those of two multipliers that have been recommended in the literature. Comparisons using packing measures in the space of k-tuples and in the dual space are also made. For modulus 2^{48}, §4 also presents analogous results for the five best multipliers and for two multipliers suggested in the literature.

Consider the multiplicative congruential random number generator

$$\{Z_0, Z_i \equiv AZ_{i-1} \pmod{M};\ i = 1, 2, \ldots\} \tag{1}$$

with multiplier A and modulus M. For the prime modulus $M = 2^{31} - 1$, Fishman and Moore [9] presented results of an exhaustive search to find those multipliers A that perform best, according to a specified criterion, on a battery of theoretical measures of randomness. The present study gives analogous results for modulus $M = 2^{32}$, commonly employed on 32 bit wordsize computers, and for $M = 2^{48}$, commonly used on CDC computers. Section 1 describes

Received November 29, 1988; revised February 13, 1989.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 65C10.
Key words and phrases. Congruential generator, discrepancy, random number generation, spectral test.
This research was supported by the Air Force Office of Scientific Research under grant AFOSR-84-0140. Reproduction in whole or part is permitted for any purpose of the United States Government.

features of this class of generators, §2 describes the theoretical measures used to assess the extent of randomness for each multiplier and §3 presents results for the best ten multipliers A out of the possible $2^{29} = 536,870,912$ candidate multipliers for $M = 2^{32}$, and for the five best multipliers among $2^{26} \approx 67.1$ million studied for $M = 2^{48}$. For each modulus, it also lists results for multipliers suggested in the literature.

1. Properties of the generator

Generators with modulus $M = 2^{\beta}$, $\beta \geq 3$, have been in common use for over thirty years. Their appeal comes from the computational efficiency that they offer on binary-word computers by replacing division and multiplication operators by shift and addition operations in the modulo reduction step in (1). If $A \equiv \pm 5 \pmod 8$, and the chosen seed Z_0 is odd, then the maximal achievable period $T = 2^{\beta-2}$ is realized before the generator repeats itself. Table 1 lists the maximal period multipliers A together with the sequences they generate for given seeds Z_0. Because of the greater uniformity over the set $\{1, \ldots, 2^{\beta-2}\}$, we chose to study $A \equiv 5 \pmod 8$. Note that all maximal period generators with $M = 2^{\beta}$ produce odd integers only.

Table 1
Multiplicative congruential generators $Z_i \equiv AZ_{i-1} \pmod M$
$(M = 2^{\beta},\ \beta \geq 3)$

A	Z_0	Generated sequence is a permutation of
5 (mod 8)	1 (mod 4)	$\{4j+1;\ j = 0, 1, \ldots, 2^{\beta-2}-1\}$
5 (mod 8)	3 (mod 4)	$\{4j+3;\ j = 0, 1, \ldots, 2^{\beta-2}-1\}$
3 (mod 8)	1 or 3 (mod 8)	$\{8j+1 \text{ and } 8j+3;\ j = 0, 1, \ldots, 2^{\beta-3}-1\}$
3 (mod 8)	5 or 7 (mod 8)	$\{8j+5 \text{ and } 8j+7;\ j = 0, 1, \ldots, 2^{\beta-3}-1\}$

Since every maximal period multiplier $A \equiv 5 \pmod 8$ belongs to the set

$$\mathscr{A} = \{5 + 8(i-1);\ i = 1, \ldots, 2^{\beta-3}\}, \tag{2a}$$

2^{29} candidate multipliers exist for $M = 2^{32}$, and 2^{45} exist for $M = 2^{48}$. Also, since

$$5^{2i-1} = 5(1 + 3 \times 8)^{i-1} \equiv 5 \pmod 8, \qquad i = 1, 2, \ldots,$$

the set $\mathscr{A}$ has the equivalent form

$$\mathscr{A} = \{5^{2i-1} \pmod{2^{\beta}};\ i = 1, \ldots, 2^{\beta-3}\}, \tag{2b}$$

which enables one to reduce the number of candidate multipliers that need to be considered.

For every sequence

$$Z_i \equiv AZ_{i-1} \pmod{2^{\beta}}, \qquad A \in \mathscr{A},\ i = 1, \ldots, 2^{\beta-2}, \tag{3}$$

there exists a reversed sequence

$$Z_{i-1} \equiv BZ_i \pmod{2^\beta}, \qquad B \in \mathscr{A}, \quad i = 1, \ldots, 2^{\beta-2}. \tag{4}$$

By direct substitution,

$$AB \equiv 1 \mod 2^\beta.$$

Let $A = 5^{2i-1} \pmod{2^\beta}$ and $B = 5^{2j-1} \pmod{2^\beta}$. Since the smallest m for which $5^m \equiv 1 \pmod{2^\beta}$ is $m = 2^{\beta-2}$, one has $2i - 1 + 2j - 1 = 2^{\beta-2}$, $i + j = 2^{\beta-3} + 1$, so that $1 \le \min(i, j) \le 2^{\beta-4}$.

Since $\{Z_i\}$ from (3) and $\{Z_i\}$ from (4) have the exact same randomness properties, it suffices to study the first $2^{\beta-4}$ candidate multipliers in (2b). For $M = 2^{32}$ there are $2^{28} = 268,435,456$ candidates, and our analysis evaluated all of them. For $M = 2^{48}$, the time to evaluate each of the $2^{44} \approx 1.76 \times 10^{13}$ multipliers is considerably greater than the corresponding time for $M = 2^{32}$. Therefore, our analysis only evaluated the first $2^{26} \approx 67.1 \times 10^6$ multipliers generated by the form (2b).

2. Theoretical measures

Let $U_i = Z_i/M$, and consider the sequence of points or *k-tuples*

$$\mathscr{V}_k = \{U_{i,k} = (U_{i+1}, \ldots, U_{i+k}); i = 1, 2, \ldots\}. \tag{5}$$

Ideally, one wants the sequence of points $\mathscr{V}_k$ to be equidistributed in the k-dimensional unit hypercube for $k = 2, 3, \ldots$. However, the form of the generator (1) limits the extent to which one can achieve this ideal. For example, observe that an ideal generator of the integers $\{4j+1;\ j = 0, 1, \ldots, 2^{\beta-2}-1\}$ produces $2^{(\beta-2)k}$ equidistributed points in the k-dimensional unit hypercube $\mathscr{H}^k$ whereas the generator (1) with $M = 2^\beta$, $A \equiv 5 \pmod 8$ and odd Z_0 produces only $T = M/4 = 2^{\beta-2}$ points in this hypercube. Hereafter, we take $M = 2^\beta$ unless otherwise specified.

2.1. **Maximal distance between parallel hyperplanes.** One way to study the distributional properties of $\mathscr{V}_k$ is through the *lattice* structure that (1) induces. It is well known that all k-tuples generated by (1) with these A and M lie on sets of hyperplanes of the form

$$\sum_{j=0}^{k-1} q_j U_{i+j} \equiv 0 \pmod 1, \qquad i = 1, \ldots, M/4, \tag{6}$$

where

$$\mathbf{q} = (q_0, \ldots, q_{k-1}) \in \{-M, -M+1, \ldots, -1, 0, 1, \ldots, M-1\}, \tag{7a}$$

$$\mathbf{q} \neq \mathbf{0}, \tag{7b}$$

$$q(A) = \sum_{j=0}^{k-1} q_j A^j \equiv 0 \pmod{M/4}, \tag{7c}$$

and where the distance between any two adjacent parallel hyperplanes is

$$d_k(\mathbf{q};\, A,\, M) = \frac{I_k(\mathbf{q})}{\left(\sum_{j=0}^{k-1} q_j^2\right)^{1/2}} \tag{8}$$

and $I_k(\mathbf{q})$ is a fixed constant. Without loss of generality (see Fishman and Moore [9, p. 29]), we restrict attention to the set $\mathscr{Q}(A) = \{\mathbf{q}: I_k(\mathbf{q}) = 1,$ satisfing (7a), (7b) and (7c)$\}$.

To assess the extent of equidistribution, one has the maximal distance between adjacent parallel hyperplanes

$$d_k^*(A,\, M) = \max_{\mathbf{q}\in\mathscr{Q}(A)} d_k(\mathbf{q};\, A,\, M) \tag{9}$$

as a worst case measure for the multiplier A in k dimensions. When using (9) to compare k-tuple performance for several alternative multipliers, one prefers the multiplier that gives the minimal distance, since this implies smaller empty regions in $\mathscr{H}^k$ for this multiplier than for the other multipliers. However, there is a limit to how small this maximal distance can be; in particular, it is known that (Cassels [4, p. 332])

$$(M/4)^{1/k} d_k^*(A,\, M) \geq \gamma_k = \begin{cases} (3/4)^{1/4}, & k = 2, \\ 2^{-1/6}, & k = 3, \\ 2^{-1/4}, & k = 4, \\ 2^{-3/10}, & k = 5, \\ (3/64)^{1/12}, & k = 6. \end{cases} \tag{10}$$

For $M = 2^{32}$ one has

$$d_k^*(A,\, 2^{32}) \geq \begin{cases} .2840 \times 10^{-4}, & k = 2, \\ .8700 \times 10^{-3}, & k = 3, \\ .4645 \times 10^{-2}, & k = 4, \\ .1269 \times 10^{-1}, & k = 5, \\ .1993 \times 10^{-1}, & k = 6. \end{cases}$$

For $M = 2^{48}$ one has

$$d_k^*(A,\, 2^{48}) \geq \begin{cases} .1109 \times 10^{-6}, & k = 2, \\ .2158 \times 10^{-4}, & k = 3, \\ .2903 \times 10^{-3}, & k = 4, \\ .1381 \times 10^{-2}, & k = 5, \\ .3814 \times 10^{-2}, & k = 6. \end{cases}$$

Originally, Coveyou and MacPherson [5] advocated the minimization of the *wave number* $1/d_k(\mathbf{q};\, A,\, M)$ and called the procedure the *spectral test.*

2.2. **Minimal number of parallel hyperplanes.** A second measure of equidistributions, suggested by Marsaglia [11], is the *number of parallel hyperplanes* $N_k(\mathbf{q}; A, M)$ that (6) induces, subject to (7), in $\mathscr{H}^k$. For a particular A, a small number indicates that there exist large regions in $\mathscr{H}^k$ that contain no k-tuples. Dieter [7] showed that the maximal number of parallel hyperplanes that intersect $\mathscr{H}^k$ is

$$N'_k(\mathbf{q}; A, M) = \sum_{j=0}^{k-1} |q_j| - 1.$$

Note that all these hyperplanes may not be occupied. A worst case measure is

$$N^*_k(A, M) = \min_{\mathbf{q}\in\mathscr{L}(A)} N'(\mathbf{q}; A, M). \tag{11}$$

For several multipliers A, one prefers the one for which $N^*_k(A, M)$ is largest. Marsaglia [11] gave the upper bound

$$N^*_k(A, M) \le [k!(M/4)]^{1/k}, \qquad k = 1, 2, \ldots,$$

so that

$$N^*_k(A, 2^{32}) \le \begin{cases} 46341, & k = 2, \\ 1861, & k = 3, \\ 401, & k = 4, \\ 167, & k = 5, \\ 96, & k = 6, \end{cases}$$

and

$$N^*_k(A, 2^{48}) \le \begin{cases} 11863284, & k = 2, \\ 75020, & k = 3, \\ 6411, & k = 4, \\ 1532, & k = 5, \\ 608, & k = 6. \end{cases}$$

Knuth [10, p. 92] pointed out that the ordering of multipliers may differ with regard to $d^*_k(A, M)$ and $N^*_k(A, M)$ in a way that justifies valuing the ordering based on $d^*_k(A, M)$ more highly. Also, see Fishman and Moore [9, p. 31].

2.3. **Distance between points.** As an alternative measure of equidistribution, Smith [18] suggested the *minimal distance* between k-tuples,

$$c^*_k(A, M) = \min_{\substack{1\le i,m\le T \\ i\ne m}} \frac{1}{M}\left[\sum_{j=0}^{k-1}(Z_{i+j} - Z_{m+j})^2\right]^{1/2}, \qquad T = 2^{\beta-2}. \tag{12}$$

Since the total number of points is fixed at T, the smaller $c^*_k(A, M)$ is for a given A, the more clustered are points in $\mathscr{H}^k$. Therefore, when comparing several multipliers in k dimensions, one prefers the one that gives the maximal $c^*_k(A, M)$. Whereas $d^*_k(A, M)$ measures distance between adjacent parallel hyperplanes in the space of the $\{Z_i\}$, $c^*_k(A, M)$ measures distance between points in this space. Since by duality, $1/c^*_k(A, M)$ is the maximal distance

between adjacent parallel hyperplanes in the $\mathbf{q}$-space, one has (Cassels [4, p. 332])

$$c_k^*(A, M) \le 1/\gamma_k (M/4)^{1/k}, \tag{13}$$

where γ_k is defined in (10). The duality also facilitates the computation of $c_k^*(A, M)$ using the algorithm in Dieter [7] for computing $d_k^*(A, M)$.

2.4. **Discrepancy.** Let

$$\mathbf{W}_{i,k} = (Z_{i+1}, \ldots, Z_{i+k}), \qquad i = 1, \ldots, T.$$

To assess equidistribution, Niederreiter [14] has proposed the discrepancy measure

$$D_N^{(k)}(A, M) = \max_{\mathscr{R}} \left| \frac{\text{number of } \mathbf{W}_{1,k}, \ldots, \mathbf{W}_{N,k} \text{ in } \mathscr{R}}{N} - \frac{\text{volume of } \mathscr{R}}{M^k} \right|, \tag{14}$$

$N = 1, \ldots, T$, where $\mathscr{R}$ ranges over all sets of points of the form $\mathscr{R} = \{(w_1, \ldots, w_r) | \alpha_1 \le w_1 < \beta_1, \ldots, \alpha_k \le w_k < \beta_k\}$. Here α_j and β_j are integers in the range $0 \le \alpha_j < \beta_j < M$ for $1 \le j \le k$, so that $\mathscr{R}$ has volume $\prod_{j=1}^{k} (\beta_j - \alpha_j)$.

Since exact computation of $D_N^{(k)}(A, M)$ is not feasible, several theoretical bounds have been proposed, principally in Niederreiter [13, 15] and Ahrens and Dieter [1]. For the case in which no member of the set $\{(M^2)^{-1}\mathbf{q}\mathbf{q}' \equiv 0 \pmod 1, \mathbf{q} \in \mathscr{Q}(A)\}$ intersects $\mathscr{R}$ and $N = T$, Ahrens and Dieter [1, Theorem 5.17] gave the computable lower bound

$$D_T^{(k)}(A, M) \ge 1 / \min_{\mathbf{q} \in \mathscr{Q}(A)} \left(\lambda_m \prod_{\substack{i=0 \\ q_i \ne 0}}^{k-1} |q_i| \right), \tag{15}$$

where m denotes the number of nonzero q_i,

$$\lambda_m = \begin{cases} m^m, & \text{if } m = 2 \text{ or } 3, \\ m^m/(m-1)^m H_m, & \text{if } m \ge 4, \end{cases}$$

$$H_m = \left[\sum_{j=0}^{\lfloor m/2 \rfloor + 1} (-1)^j \binom{m}{j} (\lfloor m/2 \rfloor + 1 - j)^{m-1}/(m-1)! \right]^m. \tag{16}$$

For $k = 2$, Niederreiter [14, 16] provided the upper bounds

$$D_T^{(2)}(A, M) \le \left(1 + \sum_{i=1}^{p} a_i\right)/T \tag{17}$$

and

$$D_T^{(2)}(A, M) \le [1 + C(K) \log T]/T, \tag{18}$$

where $a_1, \ldots, a_p$ are the partial quotients in the continued fraction expansion of $A/2^{\beta-2}$, $K = \max(a_1, \ldots, a_p)$, $C(K) = 2/\log 2$ for $1 \le K \le 3$ and

$C(K) = (K+1)/\log(K+1)$ for $K \geq 4$. Earlier, Dieter [6] derived closely related results based on continued fractions to nearest integers rather than regular continued fractions.

For $k \geq 2$ and $M = 2^\beta$ $(\beta \geq 3)$, Niederreiter [17, Theorems 4.1 and 5.2] gave the upper bound

$$D_T^{(k)}(A, M) \leq \frac{k}{M} + R^{(k)}(A, M, 2^{\beta-2}), \tag{19}$$

where

$$R^{(k)}(A, M, 2^{\beta-2}) < \frac{(2\log 2M)^k + 3(2\log 2M)^{k-1}}{(\log 2)^{k-1}\rho^{(k)}(A, 2^{\beta-2})}$$

and

$$\rho^{(k)}(A, 2^{\beta-2}) = \min_{\mathbf{q}\in\mathscr{L}(A)} \prod_{i=0}^{k-1} \max(1, 2|q_i|).$$

Unfortunately, the author became aware of these results only after a considerable amount of computation for this paper had been completed. Therefore, numerical results for (19) are not reported.

3. Analysis

This section presents results for all multipliers of the form (2b) with $M = 2^{32}$ for $i = 1, \ldots, 2^{28}$ and with $M = 2^{48}$ for $i = 1, \ldots, 2^{26}$, using an algorithm of Dieter [7], as described in Knuth [10, Algorithm S]. Because of the great number of candidates, one needs to adopt a screening procedure to identify and collect those multipliers that "perform well". For present purposes, the multipliers of most interest are those that perform well in $k = 2, \ldots, 6$ dimensions relative to the constraints that (1) imposes on all lattices in these dimensions. Consider the ratios

$$S_{1,k}(A, M) = \gamma_k / d_k^*(A, M)(M/4)^{1/k}, \qquad k = 2, \ldots, 6. \tag{20}$$

As seen from (10), $0 < S_{1,k}(A, M) \leq 1$. Now the closer $S_{1,2}(A, M), \ldots, S_{1,6}(A, M)$ are to unity, the better is the performance of this multiplier with regard to the achievable bounds in $2, \ldots, 6$ dimensions. Therefore, one way to perform the screening is to identify all multipliers for which

$$\min_{2\leq k\leq 6} S_{1,k}(A, M) \geq S, \qquad 0 < S < 1, \tag{21}$$

for specified S. Based on experience in Fishman and Moore [9], we chose $S = .80$. Note that any multiplier for which $S_{1,k}(A, M) \geq .80$ for $k = 2, \ldots, 6$ guarantees that for each k the distance between adjacent hyperplanes does not exceed the minimal achievable distance by more than 25 percent.

For $M = 2^{32}$, 132 multipliers met the criterion, implying a percentage of $100 \times 132/2^{28} = .49 \times 10^{-4}$. Of the 2^{26} multipliers studied for $M = 2^{48}$, 42 met the criterion. Assuming that these are uniformly distributed over the 2^{44} possible candidates, one concludes that about $100 \times 42/2^{26} = .63 \times 10^{-4}$ percent of the multipliers would satisfy (21), and that there are about 11 million such multipliers among the 2^{44} candidates.

TABLE 2[a]
Performance measures for selected multipliers in $Z_i \equiv AZ_{i-1} \pmod{M}$ $(M = 2^{32})$

	Multiplier $A \equiv 5^j \pmod{2^{32}}$	Exponent j		Dimension (k) 2	3	4	5	6
1.	1099087573	9649599	S_1	.8920	.8563	.8604	.8420	.8325
2.	4028795517	93795525	S_2	.8954	.7637	.6215	.6657	6576
			S_3	.8920	.8401	.8269	.7460	.8547
3.	2396548189	126371437	S_1	.8571	.9238	.8316	.8248	.8248
4.	3203713013	245509143	S_2	.7957	.7271	.7862	.6897	.6576
			S_3	.8571	.9122	.8377	.8174	.8385
5.	2824527309	6634497	S_1	.9220	.8235	.8501	.8451	.8332
6.	1732073221	96810627	S_2	.8290	.8325	.7113	.5458	.6576
			S_3	.9220	.7661	.7910	.7707	.7972
7.	3934873077	181002903	S_1	.8675	.8287	.8278	.8361	.8212
8.	1749966429	190877677	S_2	.8744	.7153	.8012	.7617	.6367
			S_3	.8675	.7825	.7393	.7531	.7329
9.	392314069	160181311	S_1	.9095	.8292	.8536	.8489	.8198
10.	2304580733	211699269	S_2	.9691	.7207	.7662	.6537	.6159
			S_3	.9095	.8061	.7869	.7932	.7923
11.	69069		S_1	.4625	.3131	.4572	.5529	.3767
	SUPER-DUPER		S_2	.4401	.2117	.3894	.5278	.3549
	Marsaglia [12, p. 275]	n.a.[b]	S_3	.4625	.5111	.5430	.5677	.5789
12.	410092949	n.a.[b]	S_1	.9121	.7670	.5725	.6612	.5842
	Borosh and		S_2	.9565	.7394	.4190	.5749	.5625
	Niederreiter [3, p. 73, $n = 30$]		S_3	.9121	.6801	.7628	.4899	.6462

[a] $S_1 = \gamma_k / d_k^*(A, M)(M/4)^{1/k}$, $S_2 = N_k^*(A, M)/(k!M/4)^{1/k}$ and $S_3 = c_k^*(A, M)\gamma_k(M/4)^{1/k}$.
[b] Not available.

For each selected multiplier and $k = 2, \ldots, 6$, we also computed the ratios

$$S_{2,k}(A, M) = N_k^*(A, M)/(k!M/4)^{1/k} \tag{22}$$

and

$$S_{3,k}(A, M) = c_k^*(A, M)\gamma_k(M/4)^{1/k}, \tag{23}$$

again using Dieter's algorithm.

We first present results for $M = 2^{32}$. Table 2 presents ratios for (20), (22), and (23) for the multipliers with the ten largest $\min_{2 \le k \le 6} S_{1,k}(A, M)$. These actually occur in pairs in which multipliers 1 and 2 have identical $\{S_{1,k}(A, M)\}$, $\{S_{2,k}(A, M)\}$, $\{S_{3,k}(A, M)\}$ and discrepancies, as do multipliers 3 and 4, etc. Although the exact reason for this commonality is not immediately clear,

TABLE 3
Packing measures in the sample space
$\omega_k(A, M) = \pi^{k/2} M[c_k^*(A, M)]^k / 4\Gamma(k/2+1)$
$(M = 2^{32})$

Multiplier A	Dimension (k) 2	3	4	5	6
1, 2	2.89	3.51	4.61	3.44	9.30
3, 4	2.67	4.49	4.86	5.43	8.30
5, 6	3.09	2.66	3.86	4.05	6.13
7, 8	2.73	2.84	2.95	3.61	3.70
9, 10	3.00	3.10	3.78	4.70	5.90
11	.78	.79	.86	.88	.90
12	3.02	1.86	3.34	.42	1.74
Upper bound	3.63	5.92	9.87	14.89	23.87

a unique relationship does exist between exponents in pairs. If the exponents are i and j, then $i+j \pmod{2^{28}} = 103445124$. Table 2 also presents results for $A = 69069$ suggested in Marsaglia [12] and called SUPER-DUPER, and for $A = 410092949$ suggested in Borosh and Niederreiter [3], who showed that among all multipliers in (2b), this A has the smallest upper bound on discrepancy for 2-tuples. A listing of the remaining 122 "best" multipliers is available from the author.

Table 2 shows that:

(a) The first ten multipliers perform considerably better than the remaining ones in the table with regard to the screening measures $S_{1,k}(A, M)$, $S_{2,k}(A, M)$ and $S_{3,k}(A, M)$.

(b) For the first ten multipliers, $S_{1,2}(A, M), \ldots, S_{1,6}(A, M)$ are remarkably close.

(c) With few exceptions, the measures $S_{3,2}(A, M), \ldots, S_{3,6}(A, M)$ are also remarkably close and behave essentially as $S_{1,2}(A, M), \ldots, S_{1,6}(A, M)$ do. As expected, $S_{1,2}(A, M) = S_{3,2}(A, M)$.

(d) $S_{2,2}(A, M), \ldots, S_{2,6}(A, M)$ show considerably more variation; no doubt a reflection of the suboptimality of these multipliers with regard to this criterion.

We now turn to another method of evaluating performance which derives from the concept of *packing* a lattice with spheres (see Cassels [4]). Recall that $c_k^*(A, M)$ is the distance between nearest points in $\mathscr{H}^k$. Then the volume of a sphere with this diameter is

$$L_k(A, M) = \frac{\pi^{k/2}[c_k^*(A, M)/2]^k}{\Gamma(k/2+1)}, \tag{24}$$

where $\Gamma(\cdot)$ denotes the gamma function. Suppose one packs the lattice with such spheres centered on each of the $M/4$ points $\mathscr{V}_k$ in (5) and at the origin. Note that these spheres merely touch and that since there are only $M/4$

TABLE 4
Packing measures in the sample space

$$\mu_k(A, M) = \frac{4\pi^{k/2}}{\Gamma(k/2+1)M[d_k^*(A, M)]^k}$$

$(M = 2^{32})$

Multiplier A	Dimension (k) 2	3	4	5	6
1, 2	2.89	3.72	5.41	6.30	7.95
3, 4	2.67	4.67	4.72	5.69	7.51
5, 6	3.09	3.31	5.15	6.42	7.99
7, 8	2.73	3.37	4.64	6.08	7.32
9, 10	3.00	3.38	5.24	6.56	7.24
11	.78	.18	.43	.77	.07
12	3.02	2.67	1.06	1.88	.95
Upper bound	3.63	5.92	9.87	14.89	23.87

TABLE 5
Bounds on discrepancy
$(M = 2^{32})$

Multiplier		Dimension (k) 2	3	4	5	6
1, 2	Lower[a]	13.09	52.30	123.0	123.0	123.0
	Upper[b]	144.4				
3, 4	Lower	14.28	57.10	57.10	57.10	301.8
	Upper	128.5				
5, 6	Lower	5.727	22.91	57.52	129.7	1250.
	Upper	65.19				
7, 8	Lower	12.74	50.96	58.83	58.83	1927.
	Upper	102.4				
9, 10	Lower	6.300	25.20	25.20	117.1	117.1
	Upper	78.23				
11	Lower	3620.	14478.	14478.	14478.	14478.
	Upper	145130.				
12	Lower	.7648	3.059	309.7	309.7	309.7
	Upper	43.77				

[a] Lower bound $= 10^9 \times 1/\min_{\mathbf{q}\in\mathcal{L}^*(A)}(\lambda_m \prod_{i=0, q_i\neq 0}^{k-1} |q_i|)$.

[b] Upper bound $= 10^9 \times (1 + \sum_{i=1}^{p} a_i)/T$.

TABLE 6[a]
Performance measures for selected multipliers in $Z_i \equiv AZ_{i-1} \pmod{M}$ $(M = 2^{48})$

	Multiplier $A \equiv 5^j \pmod{2^{48}}$	Exponent j		Dimension (k) 2	3	4	5	6
1.	68909602460261	528329	S_1	.8253	.8579	.8222	.8492	.8230
			S_2	.8370	.6336	.6547	.7290	.6165
			S_3	.8253	.8902	.7349	.8166	.8209
2.	33952834046453	8369237	S_1	.9282	.8476	.8575	.8353	.8215
			S_2	.9443	.8243	.7929	.6651	.6987
			S_3	.9282	.8964	.8631	.8134	.8089
3.	43272750451645	99279091	S_1	.8368	.8262	.8230	.8400	.8213
			S_2	.8139	.7261	.7430	.6846	.6757
			S_3	.8363	.8178	.7804	.7346	.7482
4.	127107890972165	55442561	S_1	.8531	.8193	.8216	.8495	.8224
			S_2	.8959	.5944	.6397	.7042	.5606
			S_3	.8531	.8062	.8516	.7915	.7484
5.	55151000561141	27179349	S_1	.9246	.8170	.9240	.8278	.8394
			S_2	.8449	.6128	.6703	.7029	.6428
			S_3	.9246	.8216	.8827	.7849	.8119
6.	44485709377909 (PASCLIB)	66290390456821[b]	S_1	.8269	.7416	.3983	.7307	.6177
			S_2	.8418	.6537	.3340	.6677	.5704
			S_3	.8269	.6306	.4739	.6496	.4087
7.	19073486328125[c] (Los Alamos National Laboratory)	19	S_1	.9130	.3216	.6613	.5765	.6535
			S_2	.7239	.2734	.4845	.5339	.5852
			S_3	.9130	.1503	.5299	.2737	.7714

[a] $S_1 = \gamma_k / d_k^*(A, M)(M/4)^{1/k}$, $S_2 = N_k^*(A, M)/(k!M/4)^{1/k}$ and $S_3 = c_k^*(A, M)\gamma_k(M/4)^{1/k}$.
[b] Durst [8].
[c] Beyer [2].

k-tuples, the proportion of the volume of $\mathscr{H}^k$ packed with these spheres is $ML_k(A, M)/4$. Let

$$\omega_k(A, M) = 2^k ML_k(A, M)/4. \tag{25}$$

Using the lattice packing constants in (10), one has

$$\omega_k(A, M) \leq \begin{cases} 3.63, & k = 2, \\ 5.92, & k = 3, \\ 9.87, & k = 4, \\ 14.89, & k = 5, \\ 23.87, & k = 6. \end{cases}$$

Table 3 lists $\omega_k(A, M)$ for the ten best and the two other suggested multipliers. The benefits of the ten multipliers is again apparent, since their packings are considerably better across dimensions than are those for the more commonly used multipliers.

TABLE 7

Packing measures in the sample space

$$\omega_k(A, M) = \pi^{k/2} M[c_k^*(A, M)]^k / 4\Gamma(k/2+1)$$

$$(M = 2^{48})$$

Multiplier A	Dimension (k) 2	3	4	5	6
1	2.47	4.18	2.88	5.41	7.31
2	3.13	4.26	5.48	5.30	6.69
3	2.54	3.24	3.66	3.19	4.19
4	2.64	3.10	5.19	4.63	4.19
5	3.10	3.28	5.99	4.44	6.83
6	2.48	1.48	.50	1.72	.11
7	3.02	.02	.78	.02	5.02
Upper bound	3.63	5.92	9.87	14.89	23.87

TABLE 8

Packing measures in the sample space

$$\mu_k(A, M) = \frac{4\pi^{k/2}}{\Gamma(k/2+1)M[d_k^*(A, M)]^k}$$

$$(M = 2^{48})$$

Multiplier A	Dimension (k) 2	3	4	5	6
1	2.47	3.74	4.51	6.58	7.42
2	3.13	3.60	5.34	6.06	7.34
3	2.54	3.34	4.53	6.23	7.33
4	2.64	3.10	5.19	4.63	4.19
5	3.10	3.23	7.20	5.79	8.35
6	2.48	2.41	.25	3.10	1.33
7	3.02	.49	1.89	.95	1.86
Upper bound	3.63	5.92	9.87	14.89	23.87

Knuth [10, p. 102] has also used this concept of packing to rate multipliers. However, his approach relates to packing spheres in the dual space of $q_0/M, \ldots, q_{k-1}/M$. This is done by noting that in addition to $d_k^*(A, M)$ being the maximal distance between neighboring parallel hyperplanes in the space of $\mathscr{V}_k$, the quantity $4/Md_k^*(A, M)$ is the minimal distance between points in the dual space of $q_0/M, \ldots, q_{k-1}/M$. Therefore, the volume of a sphere with radius $1/2d_k^*(A, M)$ in the dual space is

$$W_k(A, M) = \frac{\pi^{k/2}}{\Gamma(k/2+1)[2Md_k^*(A, M)]^k}. \tag{26}$$

Now observe that restrictions (7) determine that the hypercube $[-1, 1)^k$ contains exactly $(2M)^k \cdot 4/M = 2^{k+2}M^{k-1}$ k-dimensional points $\mathbf{q}/M$. Therefore,

TABLE 9
Bounds on discrepancy
($M = 2^{48}$)

Multiplier		Dimension (k) 2	3	4	5	6
1	Lower[a]	1.024	4.095	4.095	4.095	17.30
	Upper[b]	5.855				
2	Lower	.1090	.4360	.4360	3.038	3.038
	Upper	1.862				
3	Lower	.4868	1.947	1.947	1.947	8.928
	Upper	3.695				
4	Lower	.1187	.7413	.7413	.7413	37.98
	Upper	1.734				
5	Lower	.0634	.2536	.3278	.3278	.9077
	Upper	1.435				
6	Lower	.1187	1.616	1.616	1.616	28.24
	Upper	1.677				
7	Lower	.1045	12.03	12.03	12.03	12.03
	Upper	2.075				

[a] Lower bound $= 10^{12} \times 1/\min_{\mathbf{q}\in\mathcal{L}'(A)}(\lambda_m \prod_{i=0, q_i\neq 0}^{k-1} |q_i|)$.
[b] Upper bound $= 10^{12} \times (1 + \sum_{i=1}^{p} a_i)/T$.

the volume of this hypercube packed with spheres is

$$\mu_k(A, M) = 2^{k+2} M^{k-1} W_k(A, M) = \frac{4\pi^{k/2}}{\Gamma(k/2+1) M [d_k^*(A, M)]^k},$$

which is the measure of packing in the dual space. This quantity is identical with the figure of merit suggested by Knuth [10, p. 101]. Note that because of the lattice structure in the dual space, this result is invariant when the hypercube is translated by a vector of integers.

Table 4 lists $\mu_k(A, M)$ for the multipliers of interest. Again, note the better performance of the top ten. Knuth remarks that one might say that any multiplier for which $\mu_k(A, M) \geq .1$, $k = 2, \ldots, 6$, passes the spectral test, and any multiplier for which $\mu_k(A, M) \geq 1$, $k = 2, \ldots, 6$, passes the test with flying colors. By this standard, the top ten multipliers are untouchable. Table 5 presents bounds on discrepancy computed from (15) and (17).

For $M = 2^{48}$, Tables 6 through 9 present corresponding results for the five multipliers A with the largest $\min_{2\leq k\leq 6} S_{1,k}(A, M)$. It also presents results for $A = 44485709377909$, which is used in PASCLIB, a collection of utility subprograms callable from PASCAL on CDC CYBER computers, and $A = 19073486328125$ used at the Los Alamos National Laboratory (Beyer [2]). The results confirm the superiority of multipliers 1 through 5, compared to multipliers 6 and 7, as expected. A listing of the remaining 37 "best" multipliers is available from the author.

ACKNOWLEDGMENT

The author is grateful to Dr. Harald Niederreiter of the Austrian Academy of Sciences for his helpful comments on working drafts of this paper, to Dr. Louis Moore of the Rand Corporation for his assistance in obtaining the results for modulus 2^{48}, to Mr. Christos Alexopoulos of the Georgia Institute of Technology for his assistance in obtaining the results for modulus 2^{32} and to a referee whose critical comments helped improve the paper.

BIBLIOGRAPHY

1. J. H. Ahrens and U. Dieter, *Uniform random numbers*, Technical University of Graz, 1977.
2. W. Beyer, Private communication, 1988.
3. I. Borosh and H. Niederreiter, *Optimal multipliers for pseudo-random number generation by the linear congruential method*, BIT **23** (1983), 65–74.
4. J. W. S. Cassels, *An introduction to the geometry of numbers*, Springer-Verlag, New York, 1959.
5. R. R. Coveyou and R. D. MacPherson, *Fourier analysis of uniform random number generators*, J. Assoc. Comput. Mach. **14** (1967), 100–119.
6. U. Dieter, *Pseudo-random numbers: the exact distribution of pairs*, Math. Comp. **25** (1971), 855–883.
7. ——, *How to calculate shortest vectors in a lattice*, Math. Comp. **29** (1975), 827–833.
8. M. Durst, Private communication, 1989.
9. G. S. Fishman and L. R. Moore, *An exhaustive analysis of multiplicative congruential random number generators with modulus* $2^{31} - 1$, SIAM J. Sci. Statist. Comput. **7** (1986), 24–45.
10. D. E. Knuth, *The art of computer programming: Semi-numerical algorithms*, 2nd ed., Addison-Wesley, 1981.
11. G. Marsaglia, *Random numbers fall mainly in the plane*, Proc. Nat. Acad. Sci. U.S.A. **61** (1968), 25–28.
12. ——, *The structure of linear congruential sequences*, in Applications of Number Theory to Numerical Analysis (S. K. Zaremba, ed.), Academic Press, New York, 1972, pp. 249–285.
13. H. Niederreiter, *Statistical independence of linear congruential pseudo-random numbers*, Bull. Amer. Math. Soc. **82** (1976), 927–929.
14. ——, *Pseudo-random numbers and optimal coefficients*, Adv. Math. **26** (1977), 99–181.
15. ——, *The serial test for linear congruential pseudo-random numbers*, Bull. Amer. Math. Soc. **84** (1978), 273–274.
16. ——, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc. **84** (1978), 957–1041.
17. ——, *The serial test for pseudo-random numbers generated by the linear congruential method*, Numer. Math. **46** (1985), 51–68.
18. C. S. Smith, *Multiplicative pseudo-random number generators with prime modulus*, J. Assoc. Comput. Mach. **18** (1971), 586–593.

DEPARTMENT OF OPERATIONS RESEARCH, UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL, CHAPEL HILL, NORTH CAROLINA 27599-3180