BIT Numerical Mathematics **44:** 135–149, 2004.

A METHOD OF SYSTEMATIC SEARCH FOR OPTIMAL MULTIPLIERS IN CONGRUENTIAL RANDOM NUMBER GENERATORS*

F. SEZGIN[1]

[1] *Bilkent University, 06533 Bilkent, Ankara, Turkey.*
email: fatin@bilkent.edu.tr

Abstract.

This paper presents a method of systematic search for optimal multipliers for congruential random number generators. The word-size of computers is a limiting factor for development of random numbers. The generators for computers up to 32 bit word-size are already investigated in detail by several authors. Some partial works are also carried out for moduli of 2^{48} and higher sizes. Rapid advances in computer technology introduced recently 64 bit architecture in computers. There are considerable efforts to provide appropriate parameters for 64 and 128 bit moduli. Although combined generators are equivalent to huge modulus linear congruential generators, for computational efficiency, it is still advisable to choose the maximum moduli for the component generators. Due to enormous computational price of present algorithms, there is a great need for guidelines and rules for systematic search techniques. Here we propose a search method which provides 'fertile' areas of multipliers of perfect quality for spectral test in two dimensions. The method may be generalized to higher dimensions. Since figures of merit are extremely variable in dimensions higher than two, it is possible to find similar intervals if the modulus is very large.

AMS subject classification (2000): 65C10, 65Y05, 68Q22, 11A55.

Key words: lattice structure, linear congruential generators, random number, spectral test.

1 Introduction.

Random numbers are essential tools in many applications such as simulation, education, arts, numerical analysis, computer programming, recreation and sampling. Besides some physical and tabular sources, there are several deterministic computational techniques to produce random sequences of data such as congruential, shift register, lagged Fibonacci, inverse and cellular automata generators. Because of their efficiency and ease of implementation, linear congruential generators attracted the attention of many researchers. They can be used in forming combined random number generators and are especially useful for quasi Monte Carlo numerical integration.

* Received November 2002. Revised July 2003. Communicated by Åke Björck.

Mixed linear congruential generators produce a sequence of integers $\{X_i\}$ defined by the recursion

$$X_n = aX_{n-1} + c \pmod{M} \tag{1.1}$$

with appropriately defined integer constants a, c, M and initial value X_0. The special case of $c = 0$ has particular significance and is called a multiplicative congruential generator. The criteria for the choice of these constants are summarized in detail by several authors such as Fishman [10], Niederreiter [22] and Knuth [14].

Random number generators must be subjected to several theoretical and empirical tests before their use for serious applications. The spectral test is a very reliable theoretical tool to distinguish bad and good congruential generators. This test is explained in detail by Knuth [14]. Letting $0 < a < M$ and a relatively prime to M, it determines the values of

$$\nu_t = \min\left\{ \sqrt{\sum_{i=1}^{t} S_i^2} \right\} \tag{1.2}$$

for $2 \le t \le T$, given that

$$\sum_{i=1}^{t} S_i a^{i-1} \equiv 0 \pmod{M}, \tag{1.3}$$

where S_i are integers $0 \le S_i < M$, and $(S_1, \ldots, S_t) \neq (0, \ldots, 0)$. In order to make this criterion independent of M, Knuth suggests the standardized figure of merit

$$\mu_t = \frac{\pi^{t/2} \nu_t^t}{\Gamma(t/2+1) M}. \tag{1.4}$$

At present there are no definite search rules to find multipliers with satisfactory ν_t values. For small moduli it is possible to conduct an exhaustive search. Fishman and Moore [9], Fishman [11], Sezgin [25–27], Warford [28], L'Ecuyer *et al.* [18] and Kao and Wong [13] give examples of this application. For very large modulus values most authors apply random searches.

Some authors imposed several restrictions on multipliers. Some of these restrictions do not aim directly at improving the quality of the generator in spectral test. But nevertheless they reduce the number of multiplier candidates to some extent. Examples are as follows:

1. Multiplier must yield the maximum period for a multiplicative congruential generator. For example when the modulus is prime, a must be primitive element modulo M. If M is a power of 2, $a \pmod 8$ should be 5. Fishman [11] reduces the number of multiplier candidates to 1/8 of all possible candidates by using the relation $a \equiv \pm 5 \pmod 8$.
2. Once a primitive root is obtained for modulus M, Fishman [10] suggests using a^k because this is also a primitive root when k is relatively prime to

$M-1$. Dyadkin and Hamilton [5, 6] used the same property for moduli 2^{64} and 2^{128}. They investigated multipliers in the form 5^k with k odd and relatively prime to M.

3. Fishman [9] uses the multiplicative inverse for multipliers noting that for each multiplier there is an inverse a^* such that $aa^* \equiv 1 \pmod{M}$. The multipliers a and a^* produce the same sequence but in the reverse order. This property aims to find multipliers in pairs and confines the search procedure to half of the possible range. L'Ecuyer [16] used the same technique.
4. For a fast implementation in floating point arithmetic some constraints may be introduced. For example L'Ecuyer [16, 17] chooses multipliers satisfying $a(M-1) < 2^{53}$ for computers whose hardware supports the IEEE floating point arithmetic standard with at least 53 bits of precision for the mantissa.
5. By considering speed and portability, Wu [30] proposed multipliers of the form $\pm 2^{k1} \pm 2^{k2}$. Kurita [15] adopted the same approach earlier. But L'Ecuyer and Simard [19] point out statistical weaknesses of these multipliers and suggest in what context they could be used safely.
6. During the calculation of aX_{n-1} integer overflow will arise if the result exceeds the word-size of the computer. There are several ways of preventing this overflow. The best solution is to use multipliers having $[M/a] > M \pmod{a}$. For detailed explanations and examples see Wichmann and Hill [29], Sezgin [24], Park and Miller [23], and L'Ecuyer *et al.* [18].

Some approaches, however, aim to increase the efficiency of the search for high quality multipliers:

1. By considering the relation between the serial and spectral tests some authors used the continued fractions that give good results in serial test. Details and examples of this approach can be found in Borosh and Niederreiter [2], Niederrieter [21] and Brunner and Uhl [3].
2. Stern sequences may also be used for multiplier selection in two-dimensional space because of their relation to continued fractions. The readers are referred to Denzer and Ecker [4] for a general discussion of the method and details of calculation. This method is not applicable for large modulus values since it is very time consuming and requires very large computer memory.
3. A way of speeding up calculations is to use faster algorithms. For example, there are several ways of assessing the lattice structure. Entacher *et al.* [7, 8] use the LLL (Lenstra–Lenstra–Lovasz) algorithm as an efficient and reliable approximation to the spectral test.
4. If several criteria will be taken into account, it would be appropriate to start from the simple ones. For example before spectral test, prime root and implementation properties may be examined. L'Ecuyer *et al.* [18] apply Beyer quotients sequentially starting from lower dimensions and remove generators unsuccessful in any dimension from further consideration. Dyadkin and Hamilton [6] reduce the number of candidate multipliers from 105 million to 2155 by applying a five-step procedure sequentially.

We must also mention some attempts to determine optimal regions of multipliers. Specific multipliers have been proposed to improve the quality. For example the cubic lattice criterion of Marsaglia [20] yields almost cubic two-dimensional lattice. According to Ahrens *et al.* [1] the multipliers with small serial correlation can be found around the golden section number of the modulus: $a \approx (\sqrt{5}-1)M/2$. Apart from these limited attempts to determine general rules for systematic approaches, most authors rely on random searches.

In this work we will introduce some formulas expressing the figures of merit in spectral test as functions of multiplier values. We used the algorithm of Hopkins [12] for the spectral test. Let k and n be relatively prime integers and $k < n$. In Section 2, it will be shown that ν_t values will become very small when $a \approx kM/n$ with small n. Let a_y denote the multiplier obtained by moving forward and backward from this value such as $a_y = a \pm y$. Then the square of Euclidean distance for a_y, namely ${\nu_{yt}}^2$, will be expressed by a polynomial of degree $2(t-1)$. In Section 3 we derive these polynomial equations. In Section 4 we present fertile multiplier areas and a systematic method to find them. It will be shown that by using this property it is possible to determine regions of optimal multipliers. These intervals can be set up in a systematic manner and very large 'fertile' regions can be foreseen for figures of merit of spectral test especially in low dimensions. This systematic search technique is very promising for very large modulus values because the lengths of fertile regions increase with the size of the modulus.

2 Some patterns in ν_t values.

The most popular theoretical measure for assessing the quality of random number generators is the quality of distribution of t-tuples in t-dimensional space. This performance is measured by various figures of merit. The Euclidean norm ν_t is an essential criterion for the choice of good linear generators. It is instructive to investigate the distribution of this norm for various dimensions. Table 2.1 presents ν_t for a very small modulus: $M = 257$. There are several remarkable patterns in this distribution:

- The distribution is symmetrical about $M/2$. It is clear that if $S_1 + S_2 a \equiv 0 \pmod{M}$, $M-a$ will have the same ν_2 since $-S_1+S_2(M-a) \equiv 0 \pmod{M}$. Therefore either a or $M-a$ can be chosen as a multiplier provided maximum period condition is satisfied.
- Inspection of Table 2.1 reveals that minimum points exhibit a remarkable regularity. For example ν_2 becomes small when a is close to 1 (or M), $127 \approx M/2$, $86 \approx M/3$, $65 \approx M/4$, $51 \approx M/5$, $103 \approx 2M/5$, etc. There is a simple explanation for this fact: Let k and n be relatively prime integers and $k < n$. It is easy to find small integers S_1 and S_2 to obtain $S_1 + S_2 a \equiv 0 \pmod{M}$ when a is close to kM/n where n is small. In this case na will be near kM. By letting $S_2 = n$ it is possible to find $S_1 = kM - na < S_2$ minimizing ν_2. Therefore this local minimum will not exceed $(S_1^2+S_2^2)^{1/2} < (n^2+n^2)^{1/2} = n\sqrt{2}$. Maximum points, however, are more difficult to explain.

Table 2.1: The values ν_2 for multipliers which are primitive elements modulo 257.

a	ν_2	a	ν_2	a	ν_2	a	ν_2	a	ν_2	a	ν_2	a	ν_2	a	ν_2
3	3.16	40	14.32	74	8.06	97	9.43	130	3.61	161	8.54	186	14.87	218	14.76
5	5.10	41	12.53	75	13.04	101	10.30	131	5.39	163	12.53	188	16.28	219	11.40
6	6.08	43	6.08	76	14.87	102	6.40	132	7.28	164	12.08	191	8.06	220	7.28
7	7.07	45	14.32	77	10.05	103	5.10	138	13.93	166	16.28	192	5.00	224	10.63
10	10.05	47	11.40	78	13.45	105	12.08	142	11.40	167	13.34	194	6.40	229	10.30
12	12.04	48	16.28	80	16.76	106	16.76	145	14.76	170	5.00	201	13.45	230	16.40
14	14.04	51	5.39	82	11.40	107	12.04	147	7.07	171	3.16	202	14.04	233	13.04
19	16.40	53	9.43	83	8.54	108	16.28	148	10.63	172	3.61	203	13.93	237	13.34
20	13.34	54	13.93	85	3.61	109	10.63	149	16.28	174	8.54	204	9.43	238	16.40
24	13.04	55	14.04	86	3.16	110	7.07	150	12.04	175	11.40	206	5.39	243	14.04
27	16.40	56	13.45	87	5.00	112	14.76	151	16.76	177	16.76	209	16.28	245	12.04
28	10.30	63	6.40	90	13.34	115	11.40	152	12.08	179	13.45	210	11.40	247	10.05
33	10.63	65	5.00	91	16.28	119	13.93	154	5.10	180	10.05	212	14.32	250	7.07
37	7.28	66	8.06	93	12.08	125	7.28	155	6.40	181	14.87	214	6.08	251	6.08
38	11.40	69	16.28	94	12.53	126	5.39	156	10.30	182	13.04	216	12.53	252	5.10
39	14.76	71	14.87	96	8.54	127	3.61	160	9.43	183	8.06	217	14.32	254	3.16

For example ν_2 reaches peak values for $a = 19, 27, 48, 80, 91, 106, \ldots$. But there is no general pattern in these cases and, both S_1 and S_2 have significant contributions.

- It would be interesting to study the changes in ν_2 with respect to changes of a in limited ranges. For example the first seven a and ν_2 values exhibit a very strong relation. By studying larger moduli in various dimensions we observed that ν_2 can be expressed as a polynomial function of the multiplier in limited intervals. We shall develop a very fruitful search strategy using this property.

3 Polynomial functions for spectral test.

The Spectral test uses integers $\{S_1, \ldots, S_t\}$ satisfying the relation (1.3) which can be written as

$$\sum_{i=1}^{t} a^{i-1} S_i = kM \equiv 0 \pmod{M} \tag{3.1}$$

to assess the granularity of a random number generator in t-dimensional space. Let us investigate the behavior of ν_t in the neighborhood of a. Consider the neighborhood of a where the multiplier takes the value $a_y = a + y$, such that the same k value is valid. For this multiplier a_y we must have integers $(S_{y1}, \ldots, S_{yt})$ instead of $(S_1, \ldots, S_t)$ in (3.1). Therefore this equation will imply

$$\sum_{i=1}^{t} (a+y)^{i-1} S_{yi} = kM. \tag{3.2}$$

By expanding binomial terms, these equations may be expressed as

$$\sum_{i=1}^{t} S_{yi} \sum_{k=0}^{i-1} \binom{i-1}{k} y^{i-1-k} a^k = kM. \tag{3.3}$$

This expression may be rewritten by arranging terms with respect to powers of a

$$\sum_{i=0}^{t-1} a^i \sum_{k=i}^{t-1} \binom{k}{i} S_{y(k+1)} y^{k-i} = kM. \tag{3.4}$$

But this problem is already solved in (3.1) and the same solution can be adopted here. By equating coefficients of similar powers of a in expressions (3.1) and (3.4) we get

$$S_{t-k} = \sum_{i=0}^{k} \binom{t-k-1+i}{i} S_{y(t-k+i)} y^i. \tag{3.5}$$

Solving for S_{yi} we get

$$S_{y(t-k)} = \sum_{i=0}^{k} \binom{t-k-1+i}{i} S_{t-k+i} (-y)^i. \tag{3.6}$$

A proof is given in the Appendix.

Now it is possible to express ν_{yt}^2, figures of merit for $a_y = a + y$ in terms of constants used for the multiplier a. For the sake of briefness we present here only the expressions up to dimension 4. Since in two-dimensional space the definition of ν_2^2 is $\nu_2^2 = S_1^2 + S_2^2$ it is possible to write

$$\nu_{y2}^2 = S_{y1}^2 + S_{y2}^2 = S_1^2 - 2S_1S_2y + S_2^2y^2 + S_2^2 = S_2^2y^2 - 2S_1S_2y + \nu_2^2.$$

By a similar calculation:

$$\begin{aligned}
\nu_{y3}^2 &= S_3^2y^4 - 2S_2S_3y^3 + (4S_3^2 + S_2^2 + 2S_1S_3)y^2 - 2S_2(S_1 + 2S_3)y + \nu_3^2 \\
\nu_{y4}^2 &= S_4^2y^6 - 2S_3S_4y^5 + (S_3^2 + 2S_2S_4 + 9S_4^2)y^4 - 2(S_1S_4 + S_2S_3 + 6S_3S_4)y^3 + \\
&\quad + (S_2^2 + 2S_1S_3 + 4S_3^2 + 6S_2S_4 + 9S_4^2)y^2 - \\
&\quad - 2(S_1S_2 + 2S_2S_3 + 3S_3S_4)y + \nu_4^2.
\end{aligned}$$

It is clearly seen that the ν_2^2 values increase as a $2(t-1)$ degree polynomial function of y. Therefore figures of merit are more chaotic in higher dimensions. The leading term in the polynomial has crucial significance. For example in 5-dimensional space, ν^2 will increase with the eighth power of y and the peaks will be reached within narrower intervals implying shorter fertile areas and less productive search. The length of these intervals will not be larger than $M^{1/8}$.

4 Fertile areas for good multipliers.

The changes of figures of merit are very regular within certain intervals. These changes are simpler in smaller dimensions. After approaching zero near points of the form kM/n, ν_t values start to increase on both sides of these points reaching

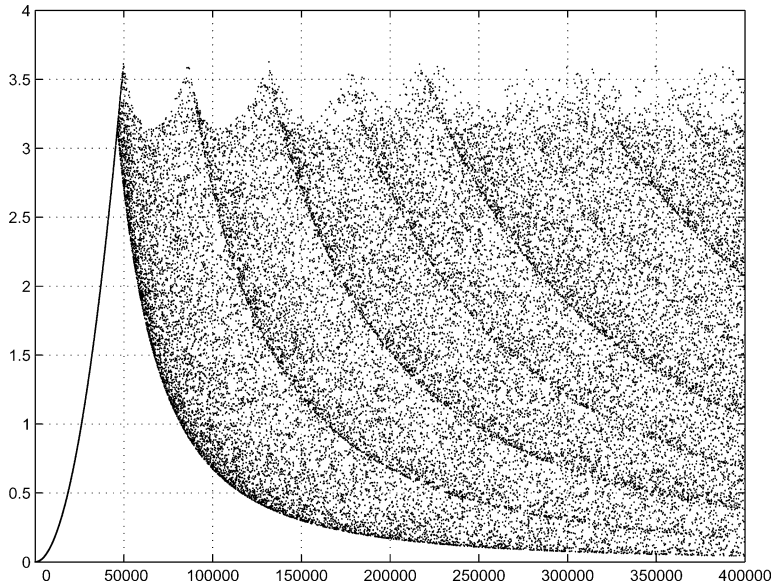

Figure 4.1: The value μ_2 peaks near $\sqrt{M}$ formed by multipliers that are primitive elements modulo $2^{31} - 1$.

a peak, and later on start to decrease. The investigation of these peaks reveals that the interval length of fertile areas has an inverse relation to n. For large n values, the curves reaching peaks are steeper and fertile areas are narrower. After the main peak, there are more peaks with gradually decreasing fertility. The distribution of μ_2 for 33213 multipliers which are primitive elements modulo $M = 2^{31} - 1$ obtained by a search in steps 3 in the interval $1 \leq a \leq 400{,}000$ is depicted in Figure 4.1.

There are remarkable patterns in the distribution. The figure has a fractal structure. The first peak $\mu_2 = 3.587$ is reached at $a = 50083 = 1.081\sqrt{M}$. The consecutive peaks have μ_2 values 3.587, 3.626, 3.528, 3.611, 3.563, 3.569, 3.586, and 3.562 corresponding to multipliers 86860, 131785, 179185, 216598, 227338, 276874, 299605 and 350302 respectively. It is interesting to remark that the quotient of these multipliers by the first peak, 50083, gives square roots of integers most of which are prime numbers: $\sqrt{3}, \sqrt{7}, \sqrt{13}, \sqrt{19}, \sqrt{21}, \sqrt{31}, \sqrt{36}, \sqrt{49}$. This property may be inspected in more detail using a greater modulus and can be used for finding some patterns for extremely large μ values. As seen in the graph an interval around the first peak will produce multipliers all having figures of merit μ_2 larger than a given threshold. For example for all multipliers $26140 \leq a \leq 82390$ we have $\mu_2 > 1.0$, similarly for $36979 \leq a \leq 52264$ we have $\mu_2 > 2.0$ and for $45289 \leq a \leq 47491$ we have $\mu_2 > 3.0$. Similar patterns will be observed for other multipliers near kM/n with small n values. For example the distribution of μ_2 near $M/2$ is very similar to Figure 4.1 but it is steeper and reaches its maximum faster: While the first curve reaches $\mu_2 = 3.0$ at the end of an interval of length 45289, the later reaches this value at the end of an interval of length 22644.

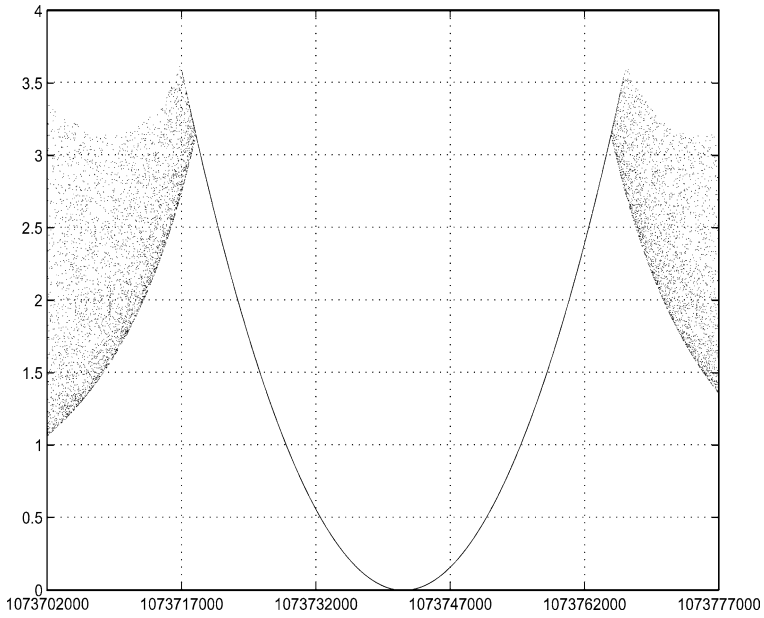

Figure 4.2: Symmetrical distributions of μ_2 around kM/n as seen for $M/2 \approx 1073741824$.

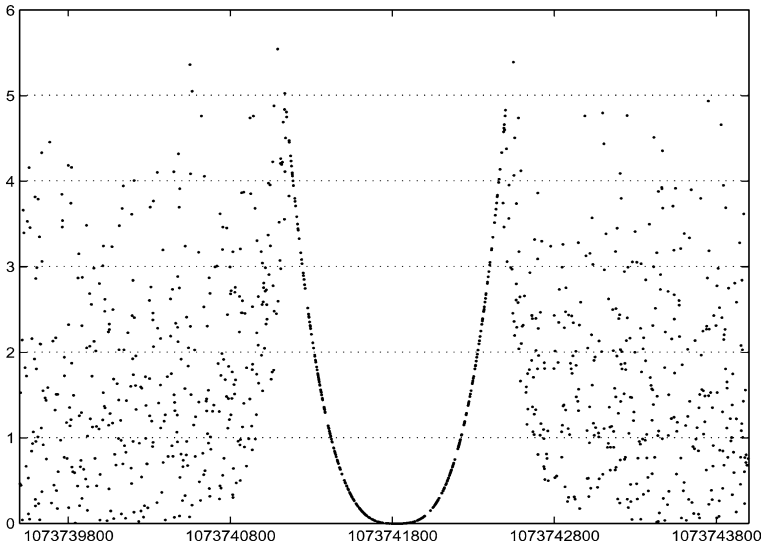

Figure 4.3: Distribution of μ_3 around $M/2$ for $M = 2147483647$.

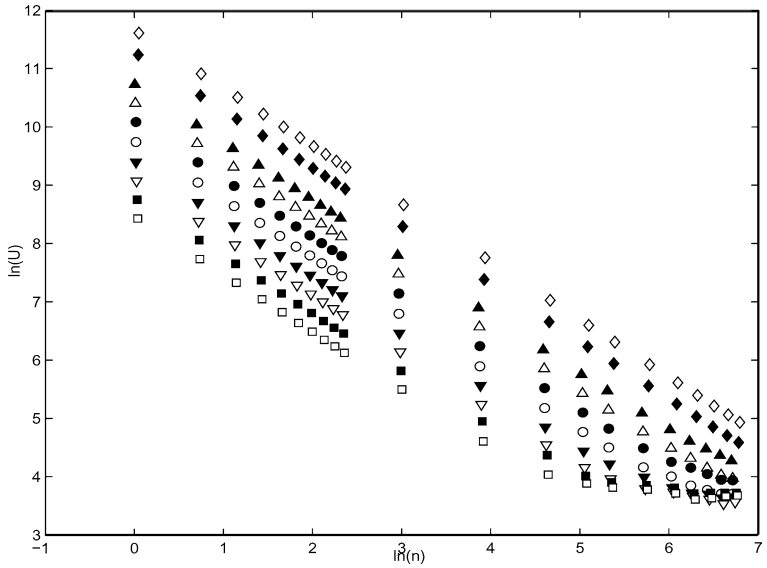

Figure 4.4: Distribution of intervals to reach from minimum μ_2 to $\mu_2 = 3.0$ for various divisors n for prime moduli between 2^{24} and 2^{33} (Modulus values from top to bottom are: 8589934583, 4294967291, 2147483647, 1073741827, 536870923, 268435459, 134217757, 67108879, 33554467, 16777213).

A perusal of Figures 4.2 and 4.3 reveals that μ_t values approach zero as the multiplier goes to $M/2$. This is a common phenomenon for multipliers of the form kM/n for small n. At the right and left sides of minimum points, μ_t starts to increase. This increase continues until μ_t reaches a maximum. For example μ_2 reaches its maxima at 1073716869 at left and 1073766925 at right. There is a distance of 50056 between these peaks. Before the first and after the second peaks there are several consecutive peaks. As in Figure 4.1, these subordinate peaks are not as fertile as the main peaks. The lower values of fluctuations get gradually smaller and smaller. Distribution of intervals U, to reach from minimum to $\mu_2 = 3.0$ for various divisors n and for prime moduli between 2^{33} and 2^{24} is presented in Figure 4.4. Figure 4.5 gives the lengths of fertile areas (Stay), for these prime moduli. The points of both graphs show strong relations. The distance to fertile area and the length of fertile area depend on divisor n through an exponential function. For example the distance from the local minimum to fertile area for modulus 8589934583 is $90138 * \exp(-0.998 * \ln(n)) \approx 90138/n$. The length of fertile area can be approximated by $3804 * \exp(-0.922 * \ln(n))$. Similar peaks are observed for higher dimensions. For example μ_3 has peaks at $a = 1073741164$ and 1073742500. The distance between maxima gets shorter with increasing t.

The relation between the divisor n and starting point of fertile area exhibits a very regular and simple form. It is possible to express this relation more concisely. Referring to the formula of figure of merit μ_t, assume that we want to find the beginning point of the fertile area where $\mu_2 > C$. This condition implies that

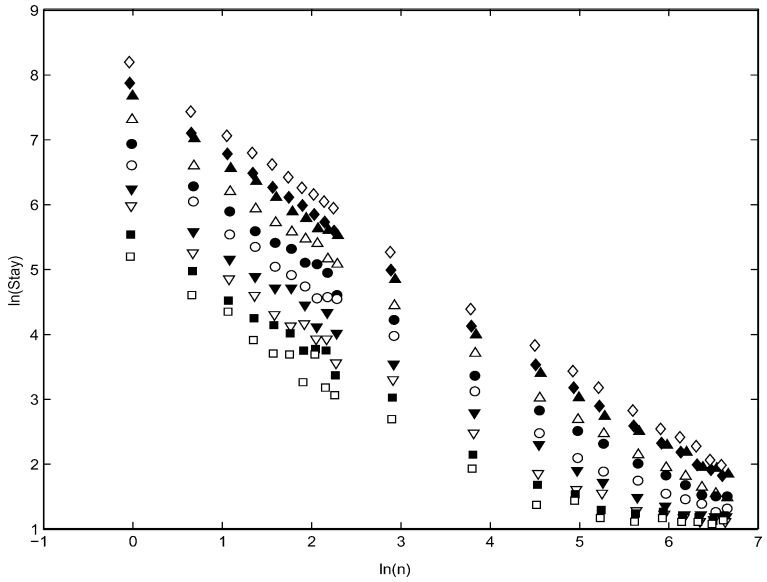

Figure 4.5: Distribution of fertile intervals for various divisors n having $\mu_2 > 3.0$ for prime moduli between 2^{24} and 2^{33} (same modulus values as in Figure 4.4).

$\nu_{y2}^2 > CM/\pi$. It is possible now to find the beginning points of fertile areas for multipliers before and after the local minimum points by solving the following inequality:

$$S_2^2 y^2 - 2S_1 S_2 y + S_1^2 + S_2^2 - CM/\pi > 0. \tag{4.1}$$

Multipliers with very small figures of merit are obtained by choosing the nearest integer to kM/n, where n is small. In Section 2 we pointed out that this would imply $S_1 = kM - na$ and $S_2 = n$. Inserting these values into the solution of (4.1) and noting that $a \approx kM/n$ we get

$$y < -\frac{1}{n}\sqrt{\frac{CM}{\pi}} \quad \text{and} \quad y > \frac{1}{n}\sqrt{\frac{CM}{\pi}}. \tag{4.2}$$

As mentioned in Section 1, Marsaglia [20] proposed the cubic lattice rule for optimum multipliers. In fact this area corresponds to the first peak of multipliers which is reached by starting from $a = 1$ and going right or starting from $M - 1$ and going left. As shown in Figure 4.1, this peak is the most fertile one and reaches its maximum at $a = 1.081\sqrt{M}$. The golden section rule of Ahrens *et al.* [1], however, does not correspond to a particular fertile area. Fertile areas near this point are extremely narrow. In fact the nearest minimum ν_2 of $a \approx (\sqrt{5} - 1)M/2$ corresponds to $2584M/4181$ approximately. We investigated an interval of length 60,000 about the golden section point and could not find a particularly fertile area. The most promising areas are quite far from the golden section point and have k/n as follows:

$$k/n = \{144/233, 233/377, 377/610, 411/665, 487/788, 500/809, 555/898\}.$$

These facts are also supported empirically by Brunner and Uhl [3] in their comparison of cubic lattice, golden section and random search strategies.

5 Application.

In application the search for fertile areas must start from smaller dimensions and go sequentially to higher dimensions. The higher dimensions must be investigated only when all lower dimensions are satisfactory. For example for the range of values investigated in Figure 4.3, although there are several multipliers satisfactory in μ_3, all these LCG's should be omitted anyway, since μ_2 is very small. Since ν_2^2 is a polynomial of degree $2(t-1)$, the figures of merit are very erratic for large dimensions when M is not extremely large. For a 32 bit modulus, the investigation of fertile regions in two dimensional space will be an efficient search strategy. In higher dimensions random searches can be conducted within these fertile areas. For 64 and higher bit moduli however, it will be worthwhile to take into account fertile regions in third and forth dimensions. This subject will be presented in a future work.

EXAMPLE 1. For $M = 2147483647$ and $n = 2$ we get $a = 1073741824$ with a very small figure of merit $\mu_2 = 5\pi/M$. The y values satisfying inequality (4.1) are $y < -13073\sqrt{C}$ and $y > 13073\sqrt{C}$. Therefore if we choose $C = 2$, it may be said that there are two fertile areas having $\mu_2 > 2.0$, the first one below $1073741824 - 18487 = 1073723337$ and the second one above $1073741824 + 18487 = 1073760311$. This agrees remarkably well with the actual calculations.

EXAMPLE 2. At present 64 bit computers are becoming more and more common. Assume that in future we will have 256 bit computers and during a search we will try to find a region of good multipliers having $\mu_2 > 3.0$ for modulus $M = 2^{256}$ near an arbitrary kM/n value such as $a \approx 71M/78942$. Then we must look below $a - y$ and above $a + y$ where

$$y = \frac{2^{128}}{78942}\sqrt{\frac{3}{\pi}}.$$

In practice the search must start from the most fertile areas and go gradually to least fertile ones. This implies starting from $n = 1$ and going to 2,3,4 etc. For $n = 1$ we choose $k = 0$ which gives the first multiplier region starting from $a = 1$ as shown in Figure 4.1. For $n = 2$, k will be equal to 1. For each n, relatively prime k values must be investigated. For $n = 3$, k is chosen as 1 and 2. Although the lengths of fertile areas decrease with n, large k numbers compensate this loss. Therefore the cumulative number of good multipliers increases as shown in Figure 5.1. But there is an upper limit for the usable n beyond which the fertile region will be so narrow that it will not be worth searching as suggested by Figure 4.5. On the other hand, by the symmetry rule mentioned in Section 2, only half of the k values need to be investigated. For example for $n = 7$, k will take values 1, 2, 3, 4, 5 and 6. Investigation of the first three k will give the necessary information for the last three.

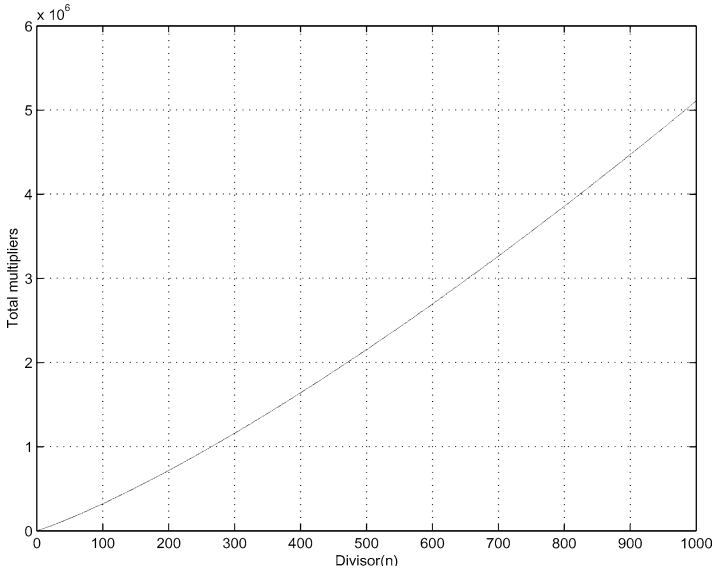

Figure 5.1: The total estimated number of multipliers having $\mu_2 > 3.0$ in two sided fertile neighborhoods of $(k/n)2147483647$ for relatively prime k and n (for $1 \leq n \leq 1000$).

The reader must be reminded that although the formulas derived here can be used to calculate spectral test values for multipliers under certain conditions, this is not the objective of this study. The aim is to speed-up computations for the search of good multipliers. For example assume that a researcher wants to find good multipliers having high figures of merit, and in particular $\mu_2 > 3$. According to our detailed experimental studies, only 7% of multipliers have this property. Considering also the symmetry property of multipliers, it is clear that the search method proposed in this study will speed up the calculations about 30 times.

6 Conclusions.

In this paper we propose a systematic search method for finding optimum multipliers for linear congruential random number generators. The Euclidean distance ν_t takes the worst value for multipliers in the form $a \approx kM/n$. But after the minima, these figures of merit recover rapidly and reach best values. We present polynomial functions expressing ν_t as a function of increases in multipliers. The method is very efficient and is capable of determining intervals where all multipliers are above a predetermined quality. The lengths of fertile areas are largest for smaller n and larger M. The search may be implemented in a sequential manner starting from smaller dimensions in spectral test. The method is very promising for random number generators suitable to larger word-size computers because the performance gets better for larger moduli. Since several n values can be investigated simultaneously, the method is also suitable for parallelization.

Appendix.

The proof is by induction. Solving (3.5) for S_{yi} we get

$$\begin{aligned} S_t &= \binom{t-1}{0} S_{yt}, \qquad S_{t-1} = \binom{t-2}{0} S_{y(t-1)} + \binom{t-1}{1} S_{yt} y, \\ S_{t-2} &= \binom{t-3}{0} S_{y(t-2)} + \binom{t-2}{1} S_{y(t-1)} y + \binom{t-1}{2} S_{yt} y^2. \end{aligned}$$

Assume that it holds for $S_{y(t-k)}$. Then it may be shown that it is valid also for $S_{y(t-k-1)}$. Since by (3.5)

$$\begin{aligned} S_{t-k-1} &= \binom{t-k-2}{0} S_{y(t-k-1)} + \binom{t-k-1}{1} S_{y(t-k)} y + \\ &\quad + \binom{t-k}{2} S_{y(t-k+1)} y^2 + \cdots + \binom{t-1}{k+1} S_{yt} y^{k+1}. \end{aligned}$$

$S_{y(t-k-1)}$ may be written as

$$\begin{aligned} S_{y(t-k-1)} &= S_{t-k-1} - \binom{t-k-1}{1} S_{y(t-k)} y - \\ &\quad - \binom{t-k}{2} S_{y(t-k+1)} y^2 - \cdots - \binom{t-1}{k+1} S_{yt} y^{k+1}. \end{aligned} \tag{A.1}$$

Since the formula is assumed to be valid for indices larger than or equal to $t-k$, we can write

$$\begin{aligned} S_{y(t-k)} &= \binom{t-k-1}{0} S_{t-k} + \binom{t-k}{1} S_{t-k+1}(-y) + \\ &\quad + \binom{t-k+1}{2} S_{t-k+2}(-y)^2 + \cdots + \binom{t-1}{k} S_t (-y)^k, \\ S_{y(t-k+1)} &= \binom{t-k}{0} S_{t-k+1} + \binom{t-k+1}{1} S_{t-k+2}(-y) + \\ &\quad + \binom{t-k+2}{2} S_{t-k+3}(-y)^2 + \cdots + \binom{t-1}{k-1} S_t (-y)^{k-1}, \\ &\vdots \\ S_{yt} &= S_t. \end{aligned}$$

By inserting these values into (A.1) and grouping with respect to powers of y, we get:

$$\begin{aligned} S_{y(t-k-1)} &= S_{t-k-1} + \binom{t-k-1}{1}\binom{t-k-1}{0} S_{t-k}(-y) + \\ &\quad + \left\{ \binom{t-k-1}{1}\binom{t-k}{1} - \binom{t-k}{2}\binom{t-k}{0} \right\} S_{t-k+1}(-y)^2 + \cdots \\ &\quad + \binom{t-1}{k+1} S_t (-y)^{k+1}. \end{aligned}$$

After some simplifications involving the multiplication of combinations, the expression reduces to

$$S_{y(t-k-1)} = S_{t-k-1} + \sum_{i=0}^{k} \frac{(t-k-1-i)!}{(t-k-2)!} S_{t-k+i}(-y)^{i+1} \sum_{j=0}^{i} \frac{(-1)^j}{(1+j)!(i-j)!}. \tag{A.2}$$

It may be shown that the second summation expression can be simplified as

$$\sum_{j=0}^{i} \frac{(-1)^j}{(1+j)!(i-j)!} = \frac{1}{(i+1)!}. \tag{A.3}$$

The proof uses the binomial expansion $(1-1)^{i+1}$. Since

$$(1-1)^{i+1} = \sum_{j=0}^{i+1} \frac{(i+1)!}{j!(i+1-j)!}(-1)^j = 0.$$

Inserting (A.3) into (A.2), we get

$$S_{y(t-k)} = \sum_{i=0}^{k} \binom{t-k+i-1}{i} S_{t-k+i}(-y)^i$$

and this completes the proof.

Acknowledgements.

I would like to thank my son Tevfik Metin Sezgin, Ph.D. student at MIT, for useful discussion concerning certain equations and contributions for the LaTeX version of the paper. I also would like to thank the two anonymous referees for their useful comments which improved the early version of the manuscript.

REFERENCES

1. J. H. Ahrens, U. Dieter, and A. Grube, *Pseudo-random numbers: A new proposal for the choice of multiplicators*, Computing, 6 (1970), pp. 121–138.
2. I. Borosh and H. Niederreiter, *Optimal multipliers for pseudo-random number generation by the linear congruential method*, BIT, 23(1) (1983), pp. 65–74.
3. D. Brunner and A. Uhl, *Optimal multipliers for linear congruential pseudo-random number generators with prime moduli: Parallel computation and properties*, BIT, 39(2) (1999), pp. 193–209.
4. V. Denzer and A. Ecker, *Optimal multipliers for linear congruential pseudo-random number generators with prime moduli*, BIT, 28 (1988), pp. 803–808.
5. I. G. Dyadkin and K. G. Hamilton, *A study of 64-bit multipliers for Lehmer pseudo-random number generators*, Comput. Phys. Comm., 103 (1997), pp. 239–258.
6. I. G. Dyadkin and K. G. Hamilton, *A study of 128-bit multipliers for congruential pseudorandom number generators*, Comput. Phys. Comm., 125 (2000), pp. 103–130.
7. K. Entacher, T. Schell, and A. A. Uhl, *Optimization of random number generators: Efficient search for high-quality LCGs*, Probab. Eng. Mech., 16 (2001), pp. 289–293.
8. K. Entacher, T. Schell, and A. A. Uhl, *Efficient lattice assessment for LCG and GLP parameter searches*, Math. Comp., 71 (2002), pp. 1231–1242.

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. Stat. Comput., 7(1) (1986), pp. 24–45.
10. G. S. Fishman, *Principles of Discrete Event Simulation*, Wiley, New York, 1987.
11. G. S. Fishman, *Multiplicative congruential random number generators with modulus* 2^{β}*: An exhaustive analysis for* $\beta = 32$ *and a partial analysis for* $\beta = 48$, Math. Comp., 54 (1990), pp. 331–344.
12. T. R. Hopkins, *Algorithm AS 193. A revised algorithm for the spectral test*, Appl. Statist., 32 (1983), pp. 328–335.
13. C. Kao and J. Y. Wong, *An exhaustive analysis of prime modulus multiplicative congruential random number generators with modulus smaller than* 2^{15}, J. Statist. Comput. Simulation, 54 (1996), pp. 29–35.
14. D. E. Knuth, *The Art of Computer Programming*, Vol. 2, 3rd ed., Addison-Wesley, Reading, MA, 1998.
15. Y. Kurita, *Choosing parameters for congruential random number generators*, in Recent Developments in Statistics, J. R. Barra *et al.*, eds., North-Holland, 1977, pp. 697–704.
16. P. L'Ecuyer, *Tables of linear congruential generators of different sizes and good lattice structure*, Math. Comp., 68 (1999), pp. 249–260.
17. P. L'Ecuyer, *Good parameters and implementations for combined multiple recursive random number generators*, Oper. Res., 47(1) (1999), pp. 159–164.
18. P. L'Ecuyer, F. Blouin, and R. Couture, *A search for good multiple recursive random number generators*, ACM Trans. on Modeling Comput. Simulation, 3(2) (1993), pp. 87–98.
19. P. L'Ecuyer and R. Simard, *Beware of linear congruential generators with multiplier* $\pm 2^q \pm 2^p$, ACM Trans. Math. Software, 25(3) (1999), pp. 367–374.
20. G. Marsaglia, *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.
21. H. Niederreiter, *Quasi-Monte Carlo methods and pseudo-random numbers*, Bull. Amer. Math. Soc., 84 (1978), pp. 957–1041.
22. H. Niederreiter, *Random Number Generation and Quasi-Monte Carlo Methods*, SIAM, Philadelphia, PA, 1992.
23. S. K. Park and K. W. Miller, *Random number generators: Good ones are hard to find*, Comm. ACM, 31(10) (1988), pp. 1192–1201.
24. F. Sezgin, *A method of obtaining portable random number generators*, in COMPSTAT'88 Computational Statistics, 8th Symposium, Copenhagen, Denmark, 1988, Physica-Verlag, Heidelberg, 1988, pp. 41–42.
25. F. Sezgin, *On a fast and portable quasi-random number generator*, Simulation Digest, 21(2) (1990), pp. 30–36.
26. F. Sezgin, *A random number generator for 16-BIT microcomputers*, Comput. Oper. Res., 23(2) (1996), pp. 193–198.
27. F. Sezgin, *Some improvements for a random number generator with single-precision floating-point arithmetic*, Comput. Geosci., 22(4) (1996), pp. 453–455.
28. J. S. Warford, *Good pedagogical random number generators*, ACM SIGCSE Bulletin, Proceedings of the twenty-third technical symposium on computer science education, 24(1) (1992), pp. 142–146.
29. B. A. Wichmann and I. D. Hill, *An efficient and portable random number generator*, Appl. Statist., 31 (1982), pp. 188–190.
30. P. Wu, *Multiplicative, congruential random number generators with multiplier* $\pm 2^{k1} \pm 2^{k2}$ *and modulus* $2^p - 1$, ACM Trans. Math. Software, 23(2) (1997), pp. 255–265.