Optimal Multipliers for the Spectral Test of Uniform Random Number Generators

Norio HARADA*

1. INTRODUCTION

In the monte carlo method, generating a reliable random number sequence is required. One of the prevailing methods of uniform random number generation is the linear congruential method, which includes the mixed ($c \neq 0$) and multiplicative ($c=0$) congruential methods:

$$x_n = a\, x_{n-1} + c \quad \mathrm{mod}\ m, \qquad (1)$$

where a, c and m are integers. We shall consider the case of multipliers giving the maximum possible periods for the mixed and multiplicative methods. R.R. Coveyou and R.D. MacPherson [2] have proposed the so-called spectral test for this method. In this paper, an algorithm of finding suitable multipliers for spectral test of Eq.(1) with $m=2^{\ell}$ and 10^{ℓ} and samples of these multipliers given by this algorithm will be shown in the following tables. These multipliers are available for practical generation of uniform random number.

Before going into the main argument, the spectral test will be briefly introduced. The spectral test claims that the magnitude of the following ν_k corresponds to good randomness of sequence generated by Eq.(1).

$$\nu^2{}_k = \min\,(S_0^2 + S_1^2 + \cdots + S_{k-1}^2) \qquad (2)$$

$$S_0 + S_1 a + \cdots\cdots + S_{k-1} a^{k-1} \equiv 0 \ \mathrm{mod}\ h, \qquad (3)$$

where h is determined by both m and whether c is equal to zero or not. Here, modulo h in Eq.(3) is as follows: (i) When $m = 2^{\ell}$ and $c = 0$, if $a \equiv -3$ mod 8, h is equal to $2^{\ell-2}$ and, if $a = 3$ mod 8, h is equal to $2^{\ell-3}$; (ii) When $m = 10^{\ell}$ and $c = 0$, h is equal to $10^{\ell}/80$; (iii) When $c \neq 0$, h is equal to m. D.E. Knuth [3] have proposed the following C_k instead of ν_k:

$$C_k = \pi^{k/2} \nu_k{}^k / ((k/2)!\,h) \qquad (4)$$

In this paper, both ν_k and C_k will be used for spectral test results.

This paper first appeared in Japanese in Joho-Shori (Journal of the Information Processing Society of Japan), Vol.15, No.3 (1974), pp.180~188.

* Central Research Laboratories, Nippon Electric Company, Limited, Kawasaki, Japan.

2. OPTIMAL MULTIPLIER

In accordance with the spectral test, the multiplier corresponds to the vector $\nu = (\nu_2, \nu_3, \ldots, \nu_k, \ldots)$. By means of this correspondence the set of multipliers can be ordered. However, since this order is not linear, it is difficult to find a multiplier with large ν_k. Generally speaking, the influence of small ν_k on the randomness of sequence by Eq.(1) is greater as k becomes smaller. Accordingly, it is reasonable to order the previous set lexicographically; that is, if $\nu_2 = \nu'_2, \ldots,$ $\nu_{k-1} = \nu'_{k-1}$ and $\nu_k > \nu'_k$, $\nu = (\nu_2, \ldots, \nu_k, \ldots)$ will be superior to $\nu' = (\nu'_2, \nu'_3, \ldots, \nu'_k, \ldots)$. This ordered set is linear. On the other hand, the inequality $\nu_k^2 \leq (4/\gamma_k^{k/2}) D^{1/k}$ is well known; where γ_k is the volume of a n-dimensional unit sphere and D is the determinant of the quadratic form deduced by Eqs. (2) and (3). In particular, $D = h^2([2])$. For example, the upper bound of C_2 is equal to 3.63. There is a maximum element in the ordered set. Conveniently, multiplier a with the maximum period will be called optimal for spectral test of Eq.(1) if the multiplier is very close to the maximum, and other ν_k (k = 3,4,..) are acceptable. There are superior multipliers which are not optimal. For example, when $c \neq 0$ and $m = 10^{11}$, a multiplier a = 39 406 980 001 has $C_2 = 3.627$, but $C_3 = 9.629 \times 10^{-3}$, $C_4 = 1.973 \times 10^{-8}$, and $C_5 = 1.579 \times 10^{-8}$.

3. ALGORITHM

An algorithm for finding the optimal multipliers will be considered. Conventionally, notations $-a$, a^{-1} and $-a^{-1}$ (mod h) imply the following integers a', a'' and a''' respectively, where $a + a' \equiv 0$, $aa'' \equiv 1$ and $aa''' \equiv -1$ mod h. These are defined as class a here.

3.1 Basic Algorithm

[Proposition 1] The values ν_k of Eq.(2) are the same among a, $-a$, a^{-1} and a^{-1}. An optimal multiplier a gives a pair of integers (n_1, n_2) with large ν_2^2, where $\nu_2^2 = n_1^2 + n_2^2$, and

$$n_1 a \equiv n_2 \mod h. \qquad (5)$$

By inverse correspondence, a pair (n_1, n_2) with large $n_1^2 + n_2^2$ will determine a multiplier with large ν_2 under the following conditions: (1) There is at least one multiplier with maximum period length in the class. (2) A pair (n_1, n_2) gives a multiplier a with $\nu_2^2 = n_1^2 + n_2^2$: that is, the value $n_1^2 + n_2^2$ is minimum among all pairs (n_1', n_2') with solution a of Eq.(5). In order to make it practical to determine superior multipliers in the above ordered set, it is sufficient to search for a pair (n_1, n_2) with large $n_1^2 + n_2^2$ which satisfy conditions (1) and (2) in the range of $T_2h/2 \leqq n_1^2 \leqq T_2h$ and $n_2^2 \leqq T_2h - n_1^2$ where $T_2 = 4/\gamma_2$.

3.2 Period Length of $-a$, a^{-1} and $-a^{-1}$.

Whether $-a$, a^{-1} and $-a^{-1}$ give the maximum period length or not for multiplier a with maximum period length is discussed.

〔Proposition 2〕 ($m = 2^{\ell}$, $\ell \geqq 5$) If multiplier a for the multiplicative congruential method with $m = 2^{\ell}$ ($\ell \geqq 5$) gives the period of maximum length, integers $-a$, a^{-1} and $-a^{-1}$ mod h $(= 2^{\ell-2})$ give maximum length. In the case of a mixed congruential method, integer a^{-1} mod h (= m) alone has the maximum length of period.

〔Proposition 3〕 Let p be a prime number of $p \equiv 1$ mod 4. If a gives the maximum period for the multiplicative method with $m = p^{\ell}$; namely if a is a primitive root modulo p^{ℓ}, then integers $-a$, a^{-1} and $-a^{-1}$ also give the maximum period.

Prop. 3 implies that, if a multiplier a of multiplicative method with $m = 10^{\ell}$ gives the maximum period length both for multiplicative methods with $m = 2^{\ell}$ and with $m=5^{\ell}$, integers $-a$, a^{-1} and $-a^{-1}$ mod h also give the maximum length for the multiplicative method with $m = 10^{\ell}$. In the case of mixed congruential method with $m = 10^{\ell}$, only a^{-1} mod 10^{ℓ} gives the maximum period, as in Prop. 2.

3.3 Choice of (n_1, n_2)

In accordance with condition (1) in 3.1, some of the class of a, which is a solution of Eq.(5) with (n_1, n_2), needs to give the maximum period length. The following propositions give the means to choose such pairs. By Prop. 1 integers n_1 and n_2 may be restricted to positive integers such that $n_1 \geqq n_2$.

〔Proposition 4〕 ($m = 2^{\ell}$, $\ell \geqq 5$) Let n_1 be odd. In the case of the multiplicative method for $m = 2^{\ell}$, all of the class of solution a in Eq.(5) with (n_1, n_2) have the maximum period length, if and only if $3n_1 \pm n_2 \equiv 0$ mod 8. And, in the case of mixed congruential method for $m = 2^{\ell}$, there are the multipliers giving the maximum period in the class of solution a of Eq.(5), if and only if $n_1 \equiv n_2$ mod 4 or $3n_1 \equiv n_2$ mod 4.

〔Proposition 5〕 ($m = 5^{\ell}$, $\ell \geqq 3$) Let n_1 and n_2 be prime to 5 and h be $5^{\ell-1}$, then solution a of Eq.(5) with (n_1, n_2) gives the maximum period length for multiplicative method with $m = 5^{\ell}$, if and only if (i) $2n_1 \equiv n_2$ mod 5 and $7n_1 \not\equiv n_2$ mod 25, or (ii) $3n_1 \equiv n_2$ mod 5 and $18n_1 \not\equiv n_2$ mod 25.

By propositions 4 and 5, a pair of integers (n_1, n_2) with maximum period length can be chosen, for multiplicative method with $m = 10^{\ell}$. For mixed congruential method,

Table 1. Optimal Multipliers of the Multiplicative and the Mixed Congruential Methods for $m = 2^{\ell}$

ℓ	No.	a, $-a$, a^{-1} and $-a^{-1}$		n_1 n_2	c_2 ν_2^2	c_3 ν_3^2	c_4 ν_4^2	c_5 ν_5^2
28	1	9,393,885 134,139,531	259,041,571 134,295,925	12,859 12,015	3.624691 309,714,106	3.008053 333,510	1.723297 9,682	1.992945 1,594
	2	473,485 1,028,421	267,961,971 267,407,035	17,575 261	3.615733 308,948,746	3.387454 361,202	3.169271 13,130	1.142182 1,272
	3	52,645,187 95,901,845	215,790,269 172,533,611	17,571 599	3.617490 309,098,842	3.855692 393,454	2.526000 11,722	3.480404 1,986
29	1	48,148,485 216,177,869	488,722,427 320,693,043	24,553 3,981	3.620419 618,698,170	2.776921 501,994	4.239422 21,476	1.906482 2,056
	2	9,665,363 240,877,349	527,205,549 295,993,563	24,829 263	3.607839 616,548,410	2.782519 503,006	3.586823 19,754	1.825337 2,034
	3	297,823,829 55,647,997	239,047,083 481,222,915	24,799 1,013	3.604727 616,016,570	2.427466 458,886	3.751359 20,202	1.344807 1,786
30	1	421,954,837 401,580,605	651,786,987 672,161,219	35,137 1,877	3.622571 1,238,131,898	2.272482 697,630	3.738779 28,522	3.085132 3,294
	2	144,014,819 380,437,365	929,527,005 693,304,459	35,135 1,891	3.622314 1,238,044,106	3.528237 935,282	3.791397 28,722	2.668940 3,118
	3	149,946,277 91,041,747	923,795,547 982,700,077	34,637 6,239	3.624078 1,238,646,890	4.240019 1,057,270	2.383683 22,774	3.055234 3,278
31	1	501,658,075 790,371,757	1,645,825,573 1,357,111,891	48,377 11,773	3.626483 2,478,937,658	2.889877 1,299,618	4.926510 46,302	4.695305 5,158
	2	1,030,999,283 502,125,509	1,116,484,365 1,645,358,139	49,765 479	3.623333 2,476,784,666	3.646602 1,517,466	4.347889 43,498	5.765088 5,600
	3	211,325,547 275,548,739	1,936,158,101 1,871,934,909	49,753 717	3.622002 2,475,875,098	3.428454 1,456,238	2.563804 33,402	4.452302 5,058
32	1	1,542,272,173 1,779,322,661	2,752,695,123 2,515,644,635	62,603 32,239	3.626931 4,958,488,730	2.313115 1,777,922	3.641630 56,298	3.985889 6,376
	2	252,989,245 1,174,634,517	4,041,978,051 3,120,332,779	62,407 32,619	3.627037 4,958,632,810	2.289628 1,766,490	5.409544 68,616	1,673156 4,514
	3	82,981,853 613,987,493	4,211,985,443 3,680,977,803	70,339 2,903	3.625113 4,956,002,330	2.053435 1,642,344	2.426367 45,954	2.810931 5,530
33	1	2,541,166,357 1,630,717,891	6,048,768,235 6,959,216,701	96,491 24,647	3.627301 9,917,987,690	3.100926 3,431,762	2.311515 63,432	2.719715 7,226
	2	4,173,311,477 2,286,409,309	4,416,623,115 6,303,525,283	77,281 62,805	3.626874 9,916,820,986	2.961650 3,327,914	3.313870 75,950	3.588125 8,066
	3	4,910,439,405 4,210,506,213	3,679,495,187 4,379,428,379	99,183 8,899	3.626742 9,916,459,690	2.939488 3,312,086	2.761674 69,334	3.367617 7,858
34	1	10,886,875,915 231,118,685	6,292,993,269 16,948,750,499	140,797 223	3.625083 19,823,844,938	3.399898 5,793,234	4.027690 118,414	1.963465 8,346
	2	9,690,319,547 713,501,299	7,489,549,637 16,466,367,885	140,771 2,769	3.625137 19,824,141,802	3.445112 5,843,570	4.352631 123,098	4.113375 11,254
	3	8,757,277,133 1,088,888,059	8,422,592,051 16,090,981,125	135,977 36,651	3.626764 19,833,040,330	3.952346 6,404,630	2.839095 99,418	1.501810 7,506
35	1	191,889,139 4,965,381,573	34,167,849,229 29,394,356,795	198,757 11,743	3.624585 39,642,243,098	3.396795 9,189,702	3.123906 147,482	2.349584 11,862
	2	1,497,111,427 6,202,832,085	32,862,626,941 28,156,906,283	198,271 18,435	3.625407 39,651,238,666	2.672721 7,832,710	4.396101 174,954	1.865937 10,822
	3	2,171,136,891 10,112,089,011	32,188,601,477 24,247,649,357	199,103 965	3.624648 39,642,935,834	3.141030 8,722,136	4.138467 169,750	1.738998 10,498
36	1	924,804,611 31,268,211,541	67,794,672,125 37,451,265,195	281,475 5,257	3.623274 79,255,811,674	3.407560 14,618,974	5.538414 277,714	2.832606 16,866
	2	267,305,339 26,431,255,987	68,452,171,397 42,288,220,749	274,821 61,465	3.625501 79,304,528,266	5.092510 19,109,222	2.619017 190,974	5.009184 21,164
	3	822,459,541 33,250,529,603	67,897,017,195 35,468,947,133	274,223 64,091	3.625564 79,305,910,010	2.771353 12,739,034	2.115173 171,624	5.014866 21,176

Table 2. Optimal Multipliers of the Multiplicative Congruential Method for $m = 10^{\ell}$

ℓ	No.	$a, -a, a^{-1}$ and $-a^{-1}$		n_1 n_2	C_2 ν_2^2	C_3 ν_3^2	C_4 ν_4^2	C_5 ν_5^2
9	1	1,199,947 2,554,717	11,300,053 9,945,283	3,771 137	3.578704 14,239,210	3.369685 46,554	2.228705 2,376	2.479804 506
	2	859,187 1,360,123	11,640,813 11,139,877	3,739 193	3.522949 14,017,370	2.056926 33,542	2.463455 2,498	1.347530 400
	3	6,356,227 3,594,837	6,143,773 8,905,163	2,883 2,441	3.586485 14,270,170	2.430725 37,390	4.012327 3,188	2.116737 478
10	1	16,773,403 12,194,067	108,226,597 112,805,933	11,633 2,901	3.612643 143,742,490	4.656932 268,282	2.334600 7,690	3.364403 1,450
	2	5,926,213 4,603,277	119,073,787 120,396,723	11,601 2,987	3.606683 143,505,370	3.152602 206,766	3.199173 9,002	5.293342 1,730
	3	37,063,427 27,288,363	87,936,573 97,711,637	9,649 7,123	3.615102 143,840,330	3.493584 221,346	5.804902 12,126	2.839604 1,350
11	1	383,889,197 63,914,533	866,110,803 1,186,085,467	37,869 1,193	3.607766 1,435,484,410	2.489215 819,890	2.277748 24,020	4.403125 4,042
	2	346,853,627 134,704,563	903,146,373 1,115,295,437	37,869 863	3.606061 1,434,805,930	2.250798 766,750	4.836659 35,002	2.770516 3,368
	3	362,235,997 10,470,667	887,764,003 1,239,529,333	37,831 2,507	3.612755 1,437,469,610	3.267553 982,952	2.146188 23,316	3.722581 3,776

the pair (n_1, n_2) such that $n_1 \equiv \pm n_2$ mod 20 give the solution with the period of maximum length.

4. EXAMPLE OF OPTIMAL MULTIPLIERS

In this section, a part of the optimal multipliers given by the previous algorithm for a short word length is shown in the form of tables as an example. Generally, many of these multipliers have better values of C_k than usual multipliers. For instance, multiplier $a = 5^{11}$ of the multiplicative method with $m = 2^{30}$ has $\nu = (2.44, 0.18, 1.43, 2.74)$. In the tables, n_1 and n_2 are defined in Eq.(5). The upper rows correspond to C_k (k=2, 3, 4, 5) and the lower rows correspond to ν_k^2 (k=2, 3, 4, 5).

4.1 Optimal Multipliers for $m = 2^{\ell}$.

Table 1 shows optimal multipliers of the multiplicative and the mixed method for $m = 2^{\ell}$. For each method, usage of Table 1 is as follows.

(1) Multiplicative Congruential Method Usage ($c = 0$)

For multiplier a with $a \equiv -3$ mod 8, modulo h of Eq.(3) is equal to $m/4 = 2^{\ell-2}$. The element with $a \equiv -3$ mod 8 in the rows of exponent $\ell-2$ in Table 1 can be regarded as candidates of multipliers for $m = 2^{\ell}$. For instance, when $m = 2^{30}$, multipliers a = 9 393 885, 134 295 925 in No. 1 of $\ell = 2^{28}$ may be optimal. By the following proposition the number of optimal multipliers from Table 1 can be increased.

〔Proposition 6〕 For multiplier a with $a = -3$ mod 8 in the multiplicative method with $m = 2^{\ell}$, all of $a + h$, $a + 2h$ and $a + 3h$ ($< m$) have the same C_k and ν_k as the

Table 3. Optimal Multipliers of the Mixed Congruential Method for $m = 10^{\ell}$

ℓ	No.	a, -a, a^{-1} and $-a^{-1}$		n_1 n_2	c_2 ν_2^2	c_3 ν_3^2	c_4 ν_4^2	c_5 ν_5^2
9	1	558,283,119 46,894,479	441,716,881 953,105,521	33,689 4,009	3.616038 1,151,020,802	2.290343 668,434	3.684868 27,326	2.807232 3,086
	2	242,150,619 262,576,979	757,849,381 737,423,021	31,563 12,503	3.620836 1,152,547,978	4.558907 1,057,686	3.898233 28,106	3.623983 3,416
	3	247,830,821 249,233,581	752,169,179 750,766,419	30,311 15,331	3.624758 1,153,796,282	2.508649 710,434	2.436013 22,218	4.707606 3,798
10	1	1,394,095,879 3,511,297,719	8,605,904,121 6,488,702,281	107,281 5,001	3.623583 11,534,222,962	2.295218 3,108,014	3.178836 80,260	2.058406 6,864
	2	86,166,859 3,008,957,539	9,913,833,141 6,991,042,461	101,199 36,059	3.625866 11,541,489,082	3.037579 3,745,706	3.913602 89,054	1.632700 6,266
	3	4,774,503,099 3,575,113,101	5,225,496,901 6,424,886,899	89,203 59,903	3.627140 11,545,544,618	2.876350 3,612,194	4.485030 95,334	5.449092 10,124
11	1	30,125,003,319 28,579,353,721	69,874,996,681 71,420,646,279	338,951 21,631	3.624006 115,355,680,562	3.939190 20,677,494	3.351598 260,610	5.105261 24,776
	2	58,109,090,481 30,750,307,921	41,890,909,519 69,249,692,079	339,773 813	3.626854 115,446,352,498	2.874097 16,759,650	4.196205 291,604	2.397395 18,300
	3	35,234,957,619 27,283,689,979	64,765,042,381 72,716,310,021	339,657 3,317	3.624703 115,377,880,138	3.705684 19,853,384	4.355461 297,086	2.022468 17,126

multiplier of a.

Prop. 6 implies that, if a is optimal, the above integers are also optimal. For instance, the integer a + h = 134 295 925 + 268 435 456 = 402 731 381 also is optimal. There are 2 x 4 x 3 = 24 candidates of multipliers with a = -3 mod 8 for one exponent ℓ in Table 1. When $a \equiv 3 \bmod 8$, h is equal to $2^{\ell-3}$. In this case, the rows of exponent $\ell - 3$ in Table 1 can be used.

(2) Mixed Congruential Method Usage ($c \neq 0$)

In this case, h is equal to m. Multipliers with $a \equiv 1 \bmod 4$ in Table 1 are the optimal multipliers for mixed congruential method. For example, when $m = 2^{30}$, multiplier a = 162 435 333 has the maximum period legnth but a = 911 306 491 does not have maximum period length. In this way, the 2 x 3 = 6 multipliers can be obtained from Table 1.

4.2 Optimal Multipliers for $m = 10^{\ell}$.

(1) Multiplicative Congruential Method Usage (c = 0)

In this case, h is equal to $10^{\ell}/80$. Table 2 shows multipliers given by the above algorithm under modulo $h = 10^{\ell}/80$. If multiplier a satisfies the following condition: $a \equiv \pm 3 \bmod 8$, $a \equiv 2, 3 \bmod 5$ and $a^4 \not\equiv 1 \bmod 25$, multiplier a has the period of maximum length modulo 10^{ℓ}. Similar to Prop. 6, integers a + sh, where s is the integers such that $0 < a + sh < m$, have the same ν_k as a. If a is optimal, integers a + sh also are optimal. For instance, multiplier a = 120 396 723 from No. 2, $\ell = 10$

of Table 2 is optimal. Therefore, a + h = 120 396 723 + 125 000 000 = 245 396 723 also is an optimal multiplier. In this way, a lot of optimal multipliers can be obtained from Table 2.

(2) Mixed Congruential Method Usage ($c \neq 0$)

Table 3 shows optimal multipliers for the mixed congruential method with $m = 10^{\ell}$. In this case, multiplier a with $a \equiv 1 \pmod{20}$ gives the maximum period length. For example, a multiplier a = 757 849 381 from No. 2, $\ell = 9$ in Table 3 is optimal, but -a = 242 150 619 is not.

5. CONCLUSION

In this paper, an algorithm to determine the suitable multiplier for the spectral test is developed by considering inverse correspondence from a pair of integers (n_1, n_2) to multiplier a. Also many multipliers for short word length are shown as tables. They are also applicable to practical uniform random number generation, since a multiplier with good ν_k is expected to give good randomness for the sequence generated by Eq.(1). For exponent ℓ, without these tables, the optimal multipliers can be calculated by this algorithm.

ACKNOWLEDGEMENT

The author would like to acknowledge the continuing guidance and encouragement of Dr. H. Watanabe, Dr. K. Ogata and Dr. T. Mikami.

REFERENCES

1. M.D. MacLaren & G. Marsaglia: Uniform Random Number Generators, JACM., Vol. 12, No. 1, pp. 83~89 (1965).
2. R.R. Coveyou & R.D. MacPherson: Fourier Analysis of Uniform Random Number Generators, JACM., Vol. 14, No. 1, pp. 100~119 (1967).
3. D.E. Knuth: The Art of Computer Programming, Vol. 2/Seminumerical Algorithms, Addison-Wesley (1969).