〈論　文〉

スペクトル検定に対する乱数列発生法の最適係数*

原　田　紀　夫**

Abstract

An algorithm finding optimal multipliers for the spectral test of uniform random number generators is developed. Many multipliers given by this algorithm are shown as the tables. They are available for practical random number generation on binary and decimal computers.

1. はじめに

現在一様乱数の発生には種々の方法がある．それらの中で最も広く用いられているのは線形合同法と呼ばれる方法であろう．これは

$$x_n \equiv a x_{n-1} + c \mod m \qquad (1)$$

なる式で作られる数列 $\{x_n\}$ を乱数列の代用に用いる方法である．この方法にはいくつかの長所もあるけれども乗数 a の決め方によっては極めて悪い統計を与えたり，連続する k 組 $(x_{i+1}, x_{i+2}, \cdots, x_{i+k})$ がある限られた少数の超平面上に乗るという現象が起こる．このように（1）の発生法には幾つか注意すべき点があるが特に乗数 a の決め方は数列 $\{x_n\}$ のランダムネス（∞ equidistribution の意味で用いる．連続する k 組の出現頻度が一様であることを k-equidistribution と呼び $k \to \infty$ を ∞-equidistribution という．）を決定づける意味で重要である．

本論文ではスペクトル検定に対して最も良い乗数 a を見出すアルゴリズムを考察し，それによって得た数表の一部を掲載する．なおスペクトル検定は k 項よりなるベクトル $(x_{i+1}, x_{i+2}, \cdots, x_{i+k})$ の出現頻度の一様性を検定するものであり，遷移確率の検定，Poker 検定などの種々の検定を含んでいると考えられるものである．したがってスペクトル検定で良い結果を与える乗数は統計的検定においても良い結果を示すことが期待される．ただし，この検定が全周期に亘ったものであること，数列のリダクションが考慮されていないことなどの点があり，表の乗数を用いる際にも対象に合致した統計的検定は不可欠である．

2. スペクトル検定について[5,9]

$0 \leqq x < 1$ の値をとる数列の一様性に関してはいわゆる Weyl の原理がある．この原理は離散値をとる数列にも拡張され，$0 \leqq x < 1$ の場合とほぼ同様な事柄が成立する．すなわち，$\{0, 1, 2, \cdots, m-1\}$ の値をとる数列 $\{x_n\}$ が k-equidistribution であるための必要十分条件は，任意の k 個の整数の組 $(s_0, s_1, \cdots, s_{k-1})$ $(\neq 0)$ に対して

$$f(s_0, s_1, \cdots, s_{k-1}) = \lim_{N \to \infty} \frac{1}{N} \sum_{i=0}^{N-1} \exp\left(\frac{-2\pi i}{m} (x_i s_0 + x_{i+1} s_1 + \cdots + x_{i+k-1} s_{k-1}) \right) \qquad (2)$$

がつねに $=0$ であることである．（1）の数列に（2）を適用するとき，簡単な計算により，どのように乗数 a を定めても（ここでは，最大周期を与える乗数に限る．）

$$s_0 + s_1 a + \cdots + s_{k-1} a^{k-1} \equiv 0 \mod h \qquad (3)$$

を満たす整数の組に対しては $(2) = 0$ が成立しないことが判る．ここで h は m と発生法によって定まる定数．簡単のためにここでは $m = 2^t$，10^t の乗法合同法のとき，$h = 2^{t-2}$，$h = 10^t/80$ とする．$m = 2^t$，10^t の混合合同法のときには $h = m$ である．R. R. Coveyou and R. D. MacPherson[5] は（3）を満たす $(s_0, s_1, \cdots, s_{k-1})$ に対して

$$\nu_k^2 = \min(s_0^2 + s_1^2 + \cdots + s_{k-1}^2) \qquad (4)$$

が大きいほど（1）で得られる数列は k-equidistribution に近いことを示した．また ν_k は m の値によって大きく変わり得るために D. E. Knuth[9] は ν_k の代わりに

---

* Optimal Multipliers for the Spectral Test of Random Number Generators, by Norio HARADA (Central Research Laboratories, Nippon Electric Co., Ltd.)

** 日本電気（株）中央研究所

$$C_k=\frac{\pi^{k/2}\nu_k{}^k}{(k/2)!\,m} \qquad (5)$$

($k=2,3,4,\cdots$) を与えている．このように（1）のランダムネスの良さを ν_k, C_k で表わすのがスペクトル検定である．

3. 最適係数

3.1 辞書式順序

2 において述べたように最大周期を与える乗数 a に対して $a\to\boldsymbol{\nu}=(\nu_2,\nu_3,\cdots,\nu_n,\cdots)$ なる対応がある．この各成分が大きな程乗数 a はスペクトル検定に関して良い．しかし，この順序では最大周期を与える乗数 a の全体は全順序とならず，これによってスペクトル検定に対して良い係数を見出すことは難しい．そこで新たな順序を考えよう．

（4）の ν_k は k が増加するにつれてつねに減少する．すなわち $\nu_2\geqq\nu_3\geqq\cdots\geqq\nu_k\geqq\cdots$ が任意の k に対して成立する．また乱数列の発生において連続する k 個の組の出現頻度が乱れるとき，k の小さい所ほど結果に大きな影響を与えると考えられる．このような観点から，ν の順序に辞書式順序を入れることは妥当なことであろう．すなわち k の小さな ν_k が大きな程ベクトル ν が大きいとする．厳密には $\boldsymbol{\nu}=(\nu_2,\nu_3,\cdots,\nu_n,\cdots)$, $\boldsymbol{\nu}'=(\nu_2',\nu_3',\cdots,\nu_n',\cdots)$ において $\nu_2=\nu_2'$, $\nu_3=\nu_3'$, $\cdots$, $\nu_{k-1}=\nu_{k-1}'$, $\nu_k>\nu_k'$, $\cdots$が成立するとき，$\nu>\nu'$ とする．

3.2 最適係数

上の順序により，乗数 a の全体は全順序集合となる．また（4）の $\nu_k{}^2$ は k 次元の正値2次形式の原点でない格子点における最小値であり，$\leqq C_nD^{1/n}$ が成立することが知られている[11]．($C_n=(4/\gamma_n{}^{n/2})$ で γ_n は単位球の体積，D は2次形式の行列式，ここでは $D=h^2$.)

したがって乗数 a には上の順序で最大の元が存在することが判る．

さてここで最適係数の定義をしよう．すなわち，(1)式の乗数 a が上の順序で最上位の元にきわめて近く，しかも ν_k（または C_k）($k=3,4,\cdots$) が許容できる程度に大きいとき，乗数 a を（1）式の**最適係数**と呼ぶことにする．(ここで許容範囲は正確には明らかでないが $C_k\geqq0.1$ であれば良いであろうといわれている[9].)

なお最適係数は同じ m に対しても乗法合同法 ($c=0$) であるか混合合同法 ($c\neq0$) であるかによって異なることに注意する必要がある．

上の順序で上位に位置し，最適係数に入らないものもある．たとえば $\bmod 10^{11}$ の混合合同法の場合，乗数 $a=39,406,980,001$ は $C_2=3.627$ で上位にあるけれども $C_3=9.629\times10^{-3}$, $C_4=1.973\times10^{-8}$, $C_5=1.579\times10^{-8}$, となり，最適係数としては不適当である．

4. 最適係数の探索アルゴリズム

ここでは最適係数を実際に導びくアルゴリズムを考察し，アルゴリズムに必要ないくつかの簡単な定理について述べる．

4.1 基本アルゴリズム

便宜的に $a+a'\equiv0 \mod h$, $aa''\equiv1 \mod h$, $aa'''\equiv-1 \mod h$ なる a', a'', a''' を $-a$, a^{-1}, $-a^{-1}$ $(\bmod h)$ で表わす．

定理 1

正整数 h に対して（3），（4）で求められる ν_k は a, $-a$, a^{-1}, $-a^{-1}$ に対してすべて等しい．

〔証明〕 $(a^{-1})^{k-1}$ を（3）の両辺に掛けることおよび $a\to-a$, $s_{2k+1}\to-s_{2k+1}$ なる置換えより明らか．
〔証終〕

定理1は明らかに一般の正整数 h において成り立つ．

さてここで最適係数の探索アルゴリズムについて述べよう．

先の順序では ν_2 が最大値をとる乗数 a が最上位となる．乗数 a に対して ν_2 が定まったと仮定すれば

$$n_1a\equiv n_2 \mod h \qquad (6)$$
$$\nu_2{}^2=n_1{}^2+n_2{}^2$$

が成り立ち，したがって乗数 a に対して整数の組 (n_1,n_2) が決定される．(一意的とは限らない.) 定理1より，n_1, n_2 を正整数に限り，しかも $n_1\geqq n_2$ と仮定してよい．これは n_1, n_2 の符号が異なれば $a\to-a$, $n_1\to-n_1$ なる置換を行ない，$|n_1|<|n_2|$ ならば（6）の両辺に a^{-1} を掛けて得られる．(a が最大周期を与えても $-a$, a^{-1}, $-a^{-1}$ が最大周期を与えるとは限らない.)

この $a\to(n_1,n_2)$ の対応の逆対応 $(n_1,n_2)\to a$ を考えることにより，アルゴリズムは次のように与えられる．すなわち基本的には $n_1{}^2+n_2{}^2\leqq C_2h$ を満たす (n_1,n_2) を定めて，それに対応する a を定めることである．このとき (n_1,n_2) から ν_2 を導くことは容易であり，大きな ν_2 をもつ (n_1,n_2) に対応する a を求めればよい．ただし (n_1,n_2) の選択には次の2点が要

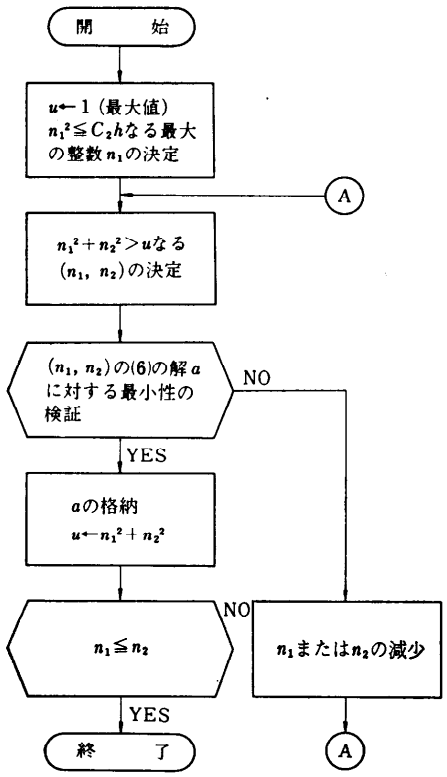

Fig. 1 Block diagram of the algorithm finding optimal multipliers.

求される.

(i) (n_1, n_2) は (6) の解 a に対して, a, $-a$, a^{-1}, $-a^{-1} (\mathrm{mod}\, h)$ の中で最大周期をもつものを含むように選択すること.

(ii) (n_1, n_2) は $n_1^2+n_2^2$ が (6) の解 a の最小値であること. すなわち (6) および $n_1'^2+n_2'^2<n_1^2+n_2^2$ を満たす (n_1', n_2') が存在しないこと.

(i) を満たす (n_1, n_2) の選択法は **4.3** で示す. (ii) に関しては a に対する最小性を検証する.

本アルゴリズムで具体的に最適係数を求めるには $C_2h/2 \leqq n_1^2 \leqq C_2h$ なる n_1 と $n_2^2 \leqq C_2h-n_1^2$ なる n_2 との組 (n_1, n_2) で (i), (ii) を満たすものを探索すればよい. このとき探索が進むに従って探索範囲を小さくすることができる. この探索範囲内で解が常に求まるという理論的根拠はなく, h が小さい場合には a が求まらない場合があるが $h \geqq 10^3$ で行なった限りでは常に解が得られた. 本アルゴリズムの流れ図を Fig. 1 に示す.

4.2 $-a$, a^{-1}, $-a^{-1}$ の最大周期性

乗数 a が最大周期を与えても $-a$, a^{-1}, $-a^{-1}$ が最大周期を与えるとは限らない. ここではおもに mod 2^l, 10^l の場合のそれらの最大周期性について議論する.

定理 2 $(m=2^l, l \geqq 5)$

正整数 a が mod 2^l の乗法合同法で最大周期を持つならば $-a$, a^{-1}, $-a^{-1} (\mathrm{mod}\, 2^{l-2})$ も最大周期をもつ. また混合合同法の場合には $a^{-1} (\mathrm{mod}\, 2^l)$ は最大周期を与え, $-a$, $-a^{-1} (\mathrm{mod}\, 2^l)$ は与えない.

〔証明〕 乗数 a が乗法合同法, 混合合同法で最大周期をもつための必要十分条件は, それぞれ $a \equiv \pm 3$ mod 8, $a \equiv 1$ mod 4 が成立することである. これより明らか. 〔証終〕

次に mod 10^l の乗法合同法に関連して次が成立する.

定理 3

p が $p \equiv 1$ mod 4 なる素数で a が mod p^l での乗法合同法で最大周期をもつならば, すなわち a が mod p^l の原始根であるならば $-a$, a^{-1}, $-a^{-1} (\mathrm{mod}\, p^l)$ もまた最大の周期をもつ.

〔証明〕 a^{-1} に関しては明らか. $-a$ に関しては次のように証明される. すなわち数列の最大周期は $\varphi(p^l)=p^{l-1}(p-1)$ で与えられる. a に関する $-a$ の巾指数は $\varphi(p^l)/2+1$ であるから $(\varphi(p^l), \varphi(p^l)/2+1)=1$ を示せばよい. $\varphi(p^l)$ と $\varphi(p^l)/2+1$ の共通因子は 1, 2 以外にない. ところが条件より $\varphi(p^l)$ は偶数, $\varphi(p^l)/2+1$ は奇数である. ここで $\varphi(p^l)$ は Euler の φ 関数, (a, b) は a, b の最大公約数を表わす. 〔証終〕

定理 3 は $p=5$ の場合, すなわち mod 5^l において乗法合同法で乗数 a が最大周期を持つならば $-a$, a^{-1}, $-a^{-1} (\mathrm{mod}\, 5^l)$ も最大周期をもつことを意味する. したがって mod 10^l の乗法合同法の場合に乗数 a を mod 2^l および mod 5^l でともに最大周期を与えるものにとれば a, $-a$, a^{-1}, $-a^{-1} (\mathrm{mod}\, 10^l)$ はすべて最大周期を与える.

mod 10^l の混合合同法の場合は定理 2 と同様に a が最大周期をもてば $a^{-1} (\mathrm{mod}\, 10^l)$ ももち, $-a$, $-a^{-1} (\mathrm{mod}\, 10^l)$ はもたないことが判る.

4.3 (n_1, n_2) の選択

4.1 で述べたように (n_1, n_2) は最大周期をもつように与えなければならない. ここでは最大周期を与える (n_1, n_2) の選択法について述べる.

定理 4 $(m=2^l, l \geqq 5)$

Table 1 Optimal multipliers of the multiplicative and the mixed congruential methods for $m=2^l$

m or h の巾数 l	No.	上段 a または $-a$ 下段 a^{-1} または $-a^{-1}$		上段 n_1 下段 n_2	上段 C_2 下段 ν_2^2	上段 C_3 下段 ν_3^2	上段 C_4 下段 ν_4^2	上段 C_5 下段 ν_5^2
28	1	9,393,885	259,041,571	12,859	3.624691	3.008053	1.723297	1.992945
		134,139,531	134,295,925	12,015	309,714,106	333,510	9,682	1,594
	2	17,681,837	250,753,619	17,489	3.625573	2.801278	2.802092	1.058692
		90,381,861	178,053,595	1,981	309,789,482	318,294	12,346	1,242
	3	473,485	267,961,971	17,575	3.615733	3.387454	3.169271	1.142182
		1,028,421	267,407,035	261	308,948,746	361,202	13,130	1,272
	4	52,645,187	215,790,269	17,571	3.617490	3.855692	2.526000	3.480404
		95,901,845	172,533,611	599	309,098,842	393,454	11,722	1,986
	5	143,208,573	125,226,883	17,481	3.621193	2.151943	3.348421	1.004841
		97,662,763	170,772,693	1,957	309,415,210	266,742	13,496	1,210
29	1	48,148,485	488,722,427	24,553	3.620419	2.776921	4.239422	1.906482
		216,177,869	320,693,043	3,981	618,698,170	501,994	21,476	2,056
	2	368,491,803	168,379,109	24,159	3.618585	3.084050	1.197081	4.705570
		233,679,597	303,191,315	5,893	618,384,730	538,526	11,412	2,954
	3	120,840,779	416,030,133	24,853	3.623424	4.099422	3.000018	0.930101
		99,068,061	437,802,851	1,241	619,211,690	651,074	18,066	1540
	4	9,665,363	527,205,549	24,829	3.607839	2.782519	3.586823	1.825337
		240,877,349	295,993,563	263	616,548,410	503,006	19,754	2,034
	5	297,823,829	239,047,083	24,799	3.604727	2.427466	3.751359	1.344807
		55,647,997	481,222,915	1,013	616,016,570	458,886	20,202	1,786
30	1	162,435,333	911,306,491	31,531	3.626122	2.412198	2.133156	2.879278
		489,722,829	584,018,995	15,657	1,239,345,610	725,746	21,544	3,210
	2	567,677,109	506,064,715	35,151	3.619663	2.574682	3.253230	1.877680
		489,792,099	583,949,725	1,243	1,237,137,850	757,734	26,626	2,714
	3	421,954,837	651,786,987	35,137	3.622571	2.272482	3.738779	3.085132
		401,580,605	672,161,219	1,877	1,238,131,898	697,630	28,522	3,294
	4	144,214,819	929,527,005	35,135	3.622314	3.528237	3.791397	2.668940
		380,437,365	693,304,459	1,891	1,238,044,106	935,282	28,722	3,118
	5	149,946,277	923,795,547	34,637	3.624078	4.240019	2.383683	3.055234
		91,041,747	982,700,077	6,239	1,238,646,890	1,057,270	22,774	3,278
31	1	501,658,075	1,645,825,573	48,377	3.626483	2.889877	4.926510	4.695305
		790,371,757	1,357,111,891	11,773	2,478,937,658	1,299,618	46,302	5,158
	2	131,571,941	2,015,911,707	49,765	3.624810	3.583600	2.126465	1.828456
		389,749,997	1,757,733,651	1,113	2,477,793,994	1,499,770	30,420	3,526
	3	1,030,999,283	1,116,484,365	49,765	3.623333	3.646602	4.347889	5.765088
		502,125,509	1,645,358,139	479	2,476,784,666	1,517,466	43,498	5,600
	4	211,325,547	1,936,158,101	49,753	3.622002	3.428454	2.563804	4.452302
		275,548,739	1,871,934,909	717	2,475,875,098	1,456,238	33,402	5,058
	5	228,125,565	1,919,358,083	49,685	3.623501	2.093676	2.909054	3.496298
		462,890,453	1,684,593,195	2,881	2,476,899,386	1,048,216	35,580	4,580
32	1	1,542,272,173	2,752,695,123	62,603	3.626931	2.313115	3.641630	3.985889
		1,779,322,661	2,515,644,635	32,239	4,958,488,730	1,777,922	56,298	6,376
	2	252,989,245	4,041,978,051	62,407	3.627037	2.289628	5.409544	1.673156
		1,174,634,517	3,120,332,779	32,619	4,958,632,810	1,766,490	68,616	4,514
	3	3,038,883,317	1,256,083,979	70,363	3.626794	2.101092	1.788150	4.723033
		2,057,972,131	2,236,995,165	2,711	4,958,301,290	1,667,454	39,450	6,814
	4	771,065,187	3,523,902,109	70,407	3.626029	2.501119	1.597012	4.684297
		311,417,781	3,983,549,515	331	4,957,255,210	1,873,278	37,282	6,786
	5	82,981,853	4,211,985,443	70,339	3.625113	2.053435	2.426367	2.810931
		613,989,493	3,680,977,803	2,903	4,956,002,330	1,642,344	45,954	5,530

m or h の巾数 l	No.	上段 a または $-a$ 下段 a^{-1} または $-a^{-1}$	上段 n_1 下段 n_2	上段 C_2 下段 ν_2^2	上段 C_3 下段 ν_3^2	上段 C_4 下段 ν_4^2	上段 C_5 下段 ν_5^2
33	1	2,541,166,357 6,048,768,235 1,630,717,891 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 4,416,623,115 2,286,409,309 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	3,313,870,693 5,276,063,899 2,039,598,483 6,550,336,109	99,545 1,891	3.625397 9,912,782,906	3.858540 3,970,242	2.409166 64,758	1.088565 5,002
	4	4,910,439,405 3,679,495,187 4,210,506,213 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
	5	729,753,035 7,860,181,557 1,609,771,037 6,980,163,555	95,357 28,703	3.626874 9,916,819,658	3.126591 3,450,854	2.573177 66,926	2.539551 7,024
34	1	10,886,875,915 6,292,993,269 231,118,685 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 7,489,549,637 713,501,299 16,466,367,885	140,771 2,769	3.625137 19,824,141,862	3.445112 5,843,570	4.352631 123,098	4.113375 11,254
	3	5,615,718,789 11,564,150,395 5,751,324,493 11,428,544,691	140,759 4,173	3.626301 19,830,510,010	2.419505 4,617,654	5.598484 139,608	0.984630 6,338
	4	8,757,277,133 8,422,592,051 1,088,888,059 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
	5	1,862,635,309 15,317,233,875 7,666,624,347 9,513,244,837	118,853 75,553	3.626993 19,834,291,418	2.283438 4,442,730	2.787246 98,506	1.542093 7,606
35	1	191,889,139 34,167,849,229 4,965,381,573 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 32,862,626,941 6,202,832,085 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	2,115,008,195 32,244,730,173 15,574,460,907 18,785,277,461	187,865 66,123	3.626712 39,665,509,354	2.794505 8,068,538	2.732198 137,926	1.196200 9,066
	4	2,171,136,891 32,188,601,477 10,112,089,011 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
	5	1,842,158,669 32,517,579,699 12,736,494,725 21,623,243,643	198,997 6,801	3.624934 39,646,059,610	1.647853 5.674,634	5.333808 192,712	2.461538 12,086
36	1	742,210,083 67,977,266,653 3,356,342,901 65,363,133,835	281,559 5,221	3.625419 79,302,729,322	2.353810 11,424,728	3.035836 205,610	2.053015 14,822
	2	213,824,629 68,505,652,107 10,313,956,317 58,405,520,419	281,531 6,263	3.625245 79,298,929,130	2.768394 12,729,002	3.742910 228,302	2.418527 15,830
	3	924,804,611 67,794,672,125 31,268,211,541 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
	4	267,305,339 68,452,171,397 26,431,255,987 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
	5	822,459,541 67,897,017,195 33,250,529,603 35,463,947,133	274,223 64,091	3.625564 79,305,910,010	2.771353 12,739,034	2.115173 171,624	5.014866 21,176

n_1 を奇数とする．乗法合同法において（6）の解 a が最大周期を与えるための必要十分条件は $3n_1 \pm n_2 \equiv 0 \mod 8$ が成立することである．ただし，$h=2^{l-2}$ とする．

また，混合合同法において（6）の解 a および $-a$，a^{-1}，$-a^{-1}$ の中に最大周期を与えるものが含まれるためには $n_1 \equiv n_2 \mod 4$ または $3n_1 \equiv n_2 \mod 4$ が成立することが必要十分である．ただし $h=m$.

〔証明〕 $a=8t\pm3$ より，$n_1(8t\pm3)=s\cdot h+n_2$，これより，$3n_1 \pm n_2 \equiv 0 \mod 8$．逆に $3n_1 \pm n_2 = 8t$ ならば $n_1 a = s\cdot h + n_2 = s\cdot h \pm 8t \mp 3n_1 = 8(h\cdot s/2^3 \pm t) \mp 3n_1$ これより $a \equiv \mp 3 \mod 8$．ここで t，s は整数．

混合合同法の場合には $a=4t+1$ より $n_1 \equiv n_2 \mod 4$，$-a=4t+3$ より $3n_1 \equiv n_2 \mod 4$．〔証終〕

次に $\mod 10^t$ の乗法合同法に関して次が成立する．

Table 2 Optimal multipliers of the multiplicative congruential method for $m=10^l$.

m の巾数 l	No.	上段 a または $-a$ 下段 a^{-1} または $-a^{-1}$		上段 n_1 下段 n^2	上段 C_2 下段 ν_2^2	上段 C_3 下段 ν_3^2	上段 C_4 下段 ν_4^2	上段 C_5 下段 ν_5^2
9	1	1,199,947	11,300,053	3,771	3.578704	3.369685	2.228705	2.479804
		2,554,717	9,945,283	137	14,239,210	46,554	2,376	506
	2	859,187	11,640,813	3,739	3.522949	2.056926	2.463455	1.347530
		1,360,123	11,139,877	193	14,017,370	33,542	2,498	400
	3	4,157,747	8,342,253	3,737	3.582846	3.052894	1.345312	5.003285
		718,917	11,781,083	539	14,255,690	43,590	1,846	676
	4	8,381,187	4,118,813	3,657	3.546614	3.695300	1.646157	2.538962
		477,877	9,022,123	859	14,111,530	49,450	2,042	512
	5	6,356,227	6,143,773	2,883	3.586485	2.430725	4.012327	2.116737
		3,594,837	8,905,163	2,441	14,270,170	37,390	3,188	478
10	1	47,903,877	77,096,123	11,891	3.603420	2.611118	3.544948	3.091731
		25,675,187	99,324,813	1,407	143,375,530	182,482	9,476	1,390
	2	16,773,403	108,226,597	11,633	3.612643	4.656932	2.334600	3.364403
		12,194,067	112,805,933	2,901	143,742,490	268,282	7,690	1,450
	3	5,926,213	119,073,787	11,601	3.606683	3.152602	3.199173	5.293342
		4,603,277	120,396,723	2,987	143,505,370	206,766	9,002	1,730
	4	37,063,427	87,936,573	9,649	3.615102	3.493584	5.804902	2.839604
		27,288,363	97,711,637	7,123	143,840,330	221,346	12,126	1,350
	5	33,097,373	91,902,627	9,253	3.615349	3.610872	2.744628	3.199417
		49,223,563	75,776,437	7,631	143,850,170	226,374	8,338	1,414
11	1	164,847,853	1,085,152,147	37,891	3.618201	3.153800	2.119395	1.243286
		567,779,483	682,220,517	1,977	1,439,636,410	960,350	23,170	2,430
	2	383,889,197	866,110,803	37,869	3.607766	2.489215	2.277748	4.403125
		63,914,533	1,186,085,467	1,193	1,435,484,410	819,890	24,020	4,042
	3	346,853,627	903,146,373	37,869	3.606061	2.250798	4.836659	2.770516
		134,704,563	1,115,295,437	863	1,434,805,930	766,750	53,002	3,368
	4	107,621,363	1,142,378,637	37,841	3.617414	2.789623	3.074802	2.737709
		322,506,427	927,493,573	2,717	1,439,323,370	884,662	27,908	3,348
	5	362,235,997	887,764,003	37,831	3.612755	3.267553	2.146188	3.722581
		10,470,667	1,239,529,333	2,507	1,437,469,610	982,952	23,316	3,776

定理5　($m=5^l, l\geqq 3$)

mod 5^l での乗法合同法で n_1, n_2 を5と互いに素とし，$h=5^{l-1}$ とする．この時（6）の解 a が最大周期をもつためには $2n_1\equiv n_2 \mod 5$ かつ $7n_1\not\equiv n_2 \mod 25$ が成立するかまたは $3n_1\equiv n_2 \mod 5$ かつ $18n_1\not\equiv n_2 \mod 25$ が成立することである．

〔証明〕 mod p^l の原始根は mod p のそれを g_0 とするとき $g=g_0+pt$ の形で，$g^{p-1}\not\equiv 1 \mod p^2$ が成立することが必要十分である．$p=5$ のとき $g_0=2$ とすれば $t\not\equiv 1 \mod 5$，$g_0=3$ とすれば $t\not\equiv 3 \mod 5$ が成立する．これより必要条件は明らか．逆に条件が成立すれば $2n_1=5k+n_2$，$n_1a=sh+n_2$ これより $n_1(a-2)=5(sh/5-k)$，したがって $a\equiv 2 \mod 5$．また，$7n_1\equiv n_2 \mod 25$，$n_1a\equiv n_2 \mod h \Leftrightarrow a\equiv 7 \mod 25$ より，$a\not\equiv 7 \mod 25$ が示される．他も同様である．〔証終〕

mod 10^l の混合合同法の場合も全く同様の方法で，(n_1, n_2) を求めることができる．すなわち $\pm a\equiv 1 \mod 4$，$\pm a\equiv 1 \mod 5$，（6）を同時に満たす (n_1, n_2) を求めればよい．

5. 最適係数表

ここでは前述のアルゴリズムで得られた最適係数の一部を掲げる．本表では紙数の関係から比較的語長の短い場合についてのみ示し，他は割愛する．これらの係数は従来の発生法に比較して良い値を与えている．

ちなみに $a=5^{11}$ $c=0$ $m=2^{30}$，$a=23$ $c\not\equiv 0$ $m=10^8+1$ の検定値はそれぞれ $\nu=(2.44,\ 0.18,\ 1.43,\ 2.74)$，$\nu=(1.67\times10^{-5},\ 5.1\times10^{-4},\ 1.39\times10^{-2},\ 3.4\times10^{-1})$ である．本表からこれらより良い値をもつ係

Table 3 Optimal multipliers of the mixed congruential method for $m=10^l$.

m の巾数 l	No.	上段 a または $-a$ 下段 a または $-a^{-1}$		上段 n_1 下段 n_2	上段 C_2 下段 ν_2^2	上段 C_3 下段 ν_3^2	上段 C_4 下段 ν_4^2	上段 C_5 下段 ν_5^2
9	1	293,770,919	706,229,081	33,761	3.622451	3.095471	2.909636	1.748356
		325,734,679	674,265,321	3,641	1,153,062,002	817,466	24,282	2,552
	2	199,300,181	800,699,819	33,723	3.619628	2.213838	2.769490	2.338032
		420,139,779	579,860,221	3,863	1,152,163,498	653,294	23,690	2,868
	3	558,283,119	441,716,881	33,689	3.616038	2.290343	3.684868	2.807232
		46,894,479	953,105,521	4,009	1,151,020,802	668,434	27,326	3,086
	4	242,150,619	757,849,381	31,563	3.620836	4.558907	3.898233	3.623983
		262,576,979	737,423,021	12,503	1,152,547,978	1,057,686	28,106	3,416
	5	247,830,821	752,169,179	30,311	3.624758	2.508649	2.436013	4.707606
		249,233,581	750,766,419	15,331	1,153,796,282	710,434	22,218	3,798
10	1	24,397,739	9,975,602,261	107,387	3.624140	4.100117	1.629867	2.904553
		1,574,489,341	8,425,510,659	2,007	11,535,995,818	4,576,114	57,470	7,874
	2	1,394,095,879	8,605,904,121	107,281	3.623583	2.295218	3.178836	2.058406
		3,511,297,719	6,488,702,281	5,001	11,534,222,962	3,108,014	80,260	6,864
	3	8,425,647,739	1,574,352,261	106,177	3.624109	3.205015	3.975368	0.924631
		2,325,739,341	7,674,260,659	16,197	11,535,898,138	3,881,994	89,754	4,974
	4	86,166,859	9,913,833,141	101,199	3.625866	3.037579	3.913602	1.632700
		3,008,957,539	6,991,042,461	36,059	11,541,489,082	3,745,706	89,054	6,266
	5	4,774,503,099	5,225,496,901	89,203	3.627140	2.876350	4.485030	5.449092
		3,575,113,101	6,424,886,899	59,903	11,545,544,618	3,612,194	95,334	10,124
11	1	30,125,003,319	69,874,996,681	338,951	3.624006	3.939190	3.351598	5.105261
		28,579,353,721	71,420,646,279	21,631	115,355,680,562	20,677,494	260,610	24,776
	2	16,780,600,639	83,219,399,361	338,939	3.619206	3.635795	1.588907	5.669121
		42,421,714,241	57,578,285,759	17,979	115,202,990,162	19,602,126	179,438	25,864
	3	549,147,361	99,450,852,639	338,899	3.623093	2.915662	2.851027	2.792415
		15,791,873,759	84,208,126,241	21,929	115,326,635,362	16,919,374	240,362	19,466
	4	58,109,090,481	41,890,909,519	339,773	3.626854	2.874097	4.196205	2.397395
		30,750,307,921	69,249,692,079	813	115,446,352,498	16,759,650	291,604	18,300
	5	35,234,957619	64,765,042,381	339,657	3.624703	3.705684	4.355461	2.022468
		27,283,689,979	72,716,310,021	3,317	115,377,880,138	19,853,384	297,086	17,126

数を見出すことは容易であろう．また C_2 の上限値は $C_2=3.63$ であり，表の係数はいずれもこの値に近いことが判る．

さて，以下に本表の概略とその使用法について述べる．表の a，$-a$，a^{-1}，$-a^{-1}$ は **4.1** で述べたものであり，上段は a または $-a$，下段は a^{-1} または $-a^{-1}$ を表わす．n_1，n_2 は（6）の係数であり，乗数の検証に用いることができる．ν_k^2，$C_k(k=2,3,4,5)$ は（4）(5）の値である．

5.1 $m=2^l$ の最適係数表

Table 1 に mod 2^l の例を示す．本表は乗法合同法，混合合同法の両方に使用することができるが使用法は異なる．以下に各場合の使用法を述べる．

（1） 乗法合同法（$c=0$）

定理2より a，$-a$，a^{-1}，$-a^{-1}(\mathrm{mod}\,h)$ はすべて最大周期を与える．ここでは簡単のために$\equiv -3 \mod 8$ なる係数に限って述べる．（$\equiv 3 \mod 8$ については〔Remark〕を参照．）このとき（3）の h は $h=m/4=2^{l-2}$ となり，本表の巾数 $l-2$ の係数の中から $\equiv -3 \mod 8$ なる係数を乗数として選ぶことができる．たとえば $m=2^{30}$ のとき巾数が 28 の No. 1 の係数 $a=9,393,885,134,295,925$ は$\equiv -3 \mod 8$ であり，乗数の候補と考えてよい．

また，$a\equiv -3 \mod 8$ なる係数 a に対して $a+h$，$a+2h$，$a+3h<m$ も a と同じ ν_k，C_k を与え，これらの係数も最適係数と考えてよい．たとえば先の例では $a=134,295,925+h=402,731,381$ も乗数の候補となる．本表によって1つの巾数に対し $2\times4\times5=40$ 個の $a\equiv -3 \mod 8$ なる乗数を作ることができる．

〔Remark〕 $a\equiv 3 \mod 8$ なる乗数においては（3）

の h は $h=2^{t-3}$ であり，しかも付帯条件 $\cos(2\pi Q(a)/m)\neq 0$ を満たす必要がある（$Q(a)$ は（3）の左辺）．したがってこの場合は巾数 $l-3$ の表から付帯条件を満たす係数を選ぶことによって最適係数を得ることができる．

このように $a\equiv 3 \mod h$ に対しては巾数 $l-2$ の表を用いることは厳密にはできないが a に対して $a+a'=m$ なる $a'\equiv -3 \mod 8$ がつねに存在して a, a' で生成される数列 $\{x_n\}$, $\{x_n'\}$ においては $x_{2n}+x_{2n}'=m$, $x_{2n+1}=x_{2n+1}'$ が成り立ち，しかも $a+a'\equiv 0 \mod h$ となる．したがってこの場合も巾数 $l-2$ の表を用いることも許容できると考えられる．いくつかの統計的検定を行なった結果は良好である．(Fig. 2, $a=259,041,571$　$m=2^{30}$ 参照.)

（2） 混合合同法（$c\neq 0$）の場合

この場合は $h=m$ であり，最適係数は最大周期性 $\equiv 1 \mod 4$ を満たすものである．たとえば $m=2^{30}$ において $l=30$, No. 1 より $a=162,435,333$ は最適係数であるが $a=911,306,491$ は最適係数ではない．本表より1つの巾数に対して $2\times 5=10$ 個の最適係数が得られる．

5.2 $m=10^t$ の最適係数表

（1） 乗法合同法（$c=0$）

この場合 $h=10^t/80$[5]* であり，Table 2 はこれによって求められたものである．（このときの付帯条件 $\sum_a \exp(-2\pi i d Q(a)/m)\neq 0$ は係数が求まって後に検証することができる．$d=1, 9, a, a^3$. $Q(a)$ は(3)の左辺.）1つの係数 a に対して $a+h$, $a+2h$, $\cdots$, $a+sh<m$ (s: 正整数) も等しい ν_t, C_t を与え，これらも最適係数と考えて良い．たとえば $l=10$, No. 3 の $a=120,396,723$ は最適係数であり，$a'=120,396,723+h=245,396,723$ も最適係数である．

（2） 混合合同法（$c\neq 0$）

Table 3 に例を掲げる．この表において，最適係数は最大周期の条件 $a\equiv 1 \mod 4$, $a\equiv 1 \mod 5$ を満たすものである．たとえば $l=9$, No. 4 において $a=757,849,381$ は最適係数であるが $a=242,150,619$ は最適係数ではない．これらの係数は表の検証に用いることが出来る．本表より $2\times 5=10$ 個の最適係数を得ることができる．

6. 統計的検定例

5 において最適係数の例を与えた．これらの係数においても 1 で述べたように使用対象や使用区間を考慮した統計的検定は必要である．ここでは最適係数の統計的検定の結果を述べるが簡単に概略することに止める．

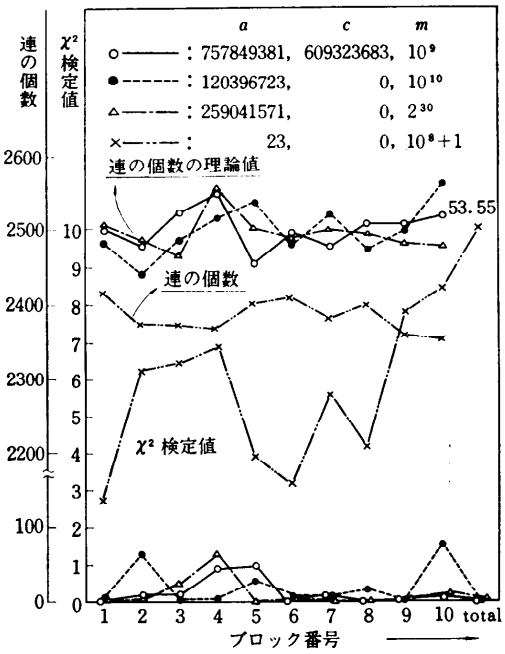

Fig. 2 Sample results of the run test.

数列はすべて $x_0=1$ で発生し，初期の 10 万個を1万個ずつのブロックに分けて検定したものであり，検定に当って $y_n=1,000\,x_n/m$ の変換を施した．検定項目は

（i） 1次元頻度検定——各数と $10(i-1)\leqq y_n<10i$ ($i=1,\cdots,2,\cdots,100$) の頻度の χ^2 検定——（ii） 2次元頻度検定——$(100(i-1)\leqq y_n<100i,\ 100(j-1)\leqq y_{n+1}<100j)$ $(i,j=1,2,\cdots,10)$ の χ^2 検定 (f. d. $=99$)——（iii） 連の検定——ここでは連の長さを平均値以上の値が連続する個数で定義し，連の個数と分布型について調べたもの——（iv）再帰時間の検定——再帰時間の分布型を調べたもの——である．

これらの検定を数十個の最適係数に対して行なった結果は出現頻度の誤差が正規分布に従うとして妥当なものであり，良好であるといってよい．

Fig. 2 に連の検定例を示す．図中の $a=23$　$c=0$　$m=10^8+1$ は最適係数ではなく，しばしば悪い例として掲げられているものである．この発生法においては（ii），（iii）が極めて悪く，（ii）では $\chi^2=443.5\sim 593.4$ (f. d. $=99$)，（iii）では Fig. 2 のとおりである．

特に Fig. 2 において連の個数が常に理論値より少ないことはこの数列から多くのサンプリングを行なえば行なう程結果が悪くなる可能性があることを示している.

7. おわりに

本論文においてスペクトル検定に対する最適係数を導びくアルゴリズムを考察し，いくつかの係数を表として掲げた．スペクトル検定は k 次元頻度 ($k \geqq 2$) の一様性を検定するものであり，これにおいて良い値を与える係数は良好な乱数列を作り出すことが期待される．しかし，乱数列の使用に際しては対象が乱数列のいかなる性質を利用するかの分析とそれに適合した各種の検定などの細心の注意が必要であり，本最適係数もそれを免れるものではない．このような観点から，本論文においても最適係数の統計的検定例について述べたけれども紙数の関係から検定の結論を概略するに止まり，結論の裏付けを十分に述べるに到らなかった．

一般にランダムネスの多くの性質を具備する乱数列を高速に作ることはこの概念から多くの異なる概念が抽象されていることから考えても難しいことと思われる．今後は使用目的に合った性質をもつ数列の発生法を考えることも重要であろう．

なお，本係数の算出には日本電気（株）中央研究所 NEAC 2200/500 を使用した．

おわりに本研究を遂行するに当って日本電気（株）中央研究所渡部部長，緒方マネジャー，三上マネジャーには多くの励ましを頂いた．また佐々木氏にはプログラムと数表の作成を手伝って頂いた．ここにこれらの方々に深く謝意を表する次第である．

参考文献

1) J. N. Franklin: Deterministic Simulation of Random Processes, Math. Comput. Vol. 17, No. 81, pp. 28～59 (1963).
2) M. D. MacLaren & G. Marsaglia: Uniform Random Number Generators, JACM., Vol. 12, No. 1, pp. 83～89 (1965).
3) R.P. Chambers: Random-number generation on digital computers, IEEE., Vol. 4, No. 2, pp. 48～56 (1967)
4) M. Greenberger: An A Priori Determination of Serial Correlation in Computer Generated Random Numbers, Math. Comput., Vol. 15, No. 76, pp. 383～389 (1961).
5) R. R. Coveyou & R. D. MacPherson: Fourier Analysis of Uniform Random Number Generators, JACM., Vol. 14, No. 1, pp. 100～119 (1967).
6) J. L. Allard, A. R. Dobell & T. E. Hull: Mixed Congruential Random Number Generators for Decimal Machines, JACM., Vol. 10, No. 2, pp. 131～141 (1963).
7) T. E. Hull & A. R. Dobell: Mixed Congruential Random Number Generators for Binary Machines, JACM., Vol. 11, No. 1, pp. 31～40 (1964).
8) D. L. Jagerman: Some Theorems Concerning Pseudo-Random Numbers, Math. Comput., Vol. 19, No. 91, pp. 418～426 (1965).
9) D. E. Knuth: The Art of Computer Programming, Vol. 2/Seminumerical Algorithms, pp. 1～160, Addison-Wesley (1969).
10) H. Griffin: Elementary Theory of Numbers, McGraw-Hill (1954).
11) 佐武：2次形式の理論，東大セミナリ・ノート II (1964).
12) 原田：スペクトル検定による乱数列発生法の最適係数，情報処理第 13 回大会予稿集，pp. 113～114 (1972).

(昭和 48 年 9 月 20 日受付)
(昭和 48 年 11 月 19 日再受付)