Constructive Design of Uniform and Independent Random Number Generators

Naoya Nakazawa[1] **and Hiroshi Nakazawa**[2]

Kronecker said: *God made natural numbers, all else is the work of man.* As inventors guess, he would have meant that the whole mathematics stood on God's invention of natural numbers, or of the recurrence relation $x_{k+1} = x_k + 1$ with $x_1 = 1$; toils, inspirations and thoughts of excellent people thereafter enabled us to have rationals, reals, complex numbers, matrices, geometry, analysis, and the algebraic systems among others. Inventors at present are in the extreme distance from the state to appreciate the depth and beauties of these mathematics of our day. Yet the perspective, that the whole system of mathematics is built from the simplest recursive relation, encourages us. We present here ways of constructing excellent generators of uniform and independent random numbers on computers. A plain fact working behind computers is that any *finite* sequence $\{u_k|\ 0 < u_k < 1,\ k = 1, 2, \cdots, T\}$ of uniformly bounded real numbers may be regarded as obtained by a multiplicative congruential method. We put this to the basis of the technological way to generate random numbers. Certainly, this deed seems not defying Gods, as they bless human graciously by allowing for the disclosure of some of their integers of brilliant performances.

1. Introduction

As the use of distilled water without impurities is indispensable to secure stable and accurate chemical transformations, random numbers with various statistics are obtained on computers by highly accurate analytic transformations, but only from purely uniform and independent ones. The generation of random numbers with highly accurate uniformity and independence is thus vital to theories and any computer simulations that utilize various types of random numbers. The aim of this report is to present inventions for methods to generate random number sequences on computers with radically improved accuracy in their statistics. It should be noted that theories of probability or stochastic processes invariably rest on premises that sequences consist of infinite elements and that numbers treated have infinite precision of real numbers . They bring in many simplifications as well as unifications, typically in forms of limit theorems or ergodic theorems. In contrast, computers can treat only a finite length T for the sequence, however large T might be. And their *real* numbers can only be discrete with the smallest unit of precision. Finiteness of sequences and discreteness of numbers usually raise complications. Yet, our conscious use of finiteness and discreteness frees us from various metaphysical problems, such as the question of the possibility of generation itself of random numbers on computers.

[1]nmail@nakazawa-patents.jp
[2]nmail@nakazawa-patents.jp

We proceed here assuming explicitly the finiteness of treated numbers and sequences. As will be elucidated shortly, this enables us to concentrate on the multiplicative and congruential generation of uniform and independent random numbers, which comprises

a positive integer d called modulus,

a positive integer z called multiplier coprime to d, and

a positive integer n called initial value or seed also coprime to d,

emits a sequence $\{r_k \equiv nz^k \bmod (d) |\ 0 < r_k < d,\ k = 0, 1, 2, \cdots\}$ of integers recursively by congruence relations

$$r_0 \equiv n \bmod (d), \quad r_{k+1} \equiv zr_k \bmod (d), \quad 0 < r_k < d, \ \ k = 0, 1, 2, \cdots,$$

and gives the sequence $\{v_1, v_2, v_3, \cdots\}$ for random numbers in the interval $(0, 1)$ as

$$\{v_k = r_{k-1}/d |\ \ k = 1, 2, 3, \cdots\}.$$

Note the staggered definition of v_k and r_{k-1} adopted here for some later conveniences. A multiplicative congruential generator for uniform and independent random numbers with the modulus d, the multiplier z and the initial value n will be noted symbolically as (d, z, n). If the initial value n is not relevant in arguments, the symbol will be shortened to (d, z). It is not that the information of random numbers is compressed into three numbers (d, z, n); it is the totality of prescriptions given by (d, z, n) *and* the vast amount of ensuing computational works to obtain the sequence: Can we judge, or even only guess, which set of three integers (d, z, n) will give a good or bad sequence of random numbers without toilsome and time-consuming computation, say of spectral tests? The answer is definitely no.

2. Description of the Related Art

We start with the general mathematical and technological characterization of the problem. Generators of random numbers on computers are required to be reproducible, i.e. they should give the identical sequence of random numbers on demands of users, typically in their need to debug simulation programs. Generators should also be transportable, i.e. they should reproduce the identical sequence of random numbers on any computers and in any computing languages. And simulations usually require too many random numbers to be stored in the computer memory. Thus, random numbers on computers can only be generated successively by the integer arithmetic, which is free from truncation and round-off errors, gives the identical results on any computers or in any computing languages, or even after any number of times of computation. Thus, computers should produce a sequence $\{x_1, x_2, \cdots, x_T\}$ of *integers* bounded as $0 \leq x_k < z$ for all k with a sufficiently

large integer z, and emit $u_k := x_k/z$ successively for $k = 1, 2, \cdots$ as uniform and independent random numbers finally by the real or rational arithmetic. The number of different states, in any computer available for the determination of the next integer output, is finite. Hence its initial state inevitably recurs, and the length of the random number sequence specified by T is restricted to be finite. Let $\{x_1, x_2, \cdots, x_T\}$ be an arbitrary finite sequence of integers within a bound $0 \le x_k < z$. Excluding two cases that $\{x_1, x_2, \cdots, x_T\}$ are all zero and all $d-1$, we have a simple circumstance that this sequence corresponds to a period of the periodic sequence arising in the division process of an irreducible fraction $x := n/d$ with $0 < n < d$ or $1 < x < 1$ to the base z,

$$x = 0.x_1x_2\cdots x_Tx_1x_2\cdots x_T\cdots = (x_1z^{T-1} + x_2z^{T-2} + \cdots x_T)/(z^T - 1) = n/d.$$

Since the divisor d is a factor of $z^T - 1$, d and z are coprime. Division processes of n over d never end, and are expressed by equations starting from $r_0 \equiv n \bmod (d)$,

$$zr_{k-1} = dx_k + r_k, \;\; 1 \le r_k < d, \;\; 0 \le x_k < z, \;\; r_k \equiv zr_{k-1} \bmod (d), \;\; k = 1, 2, 3, \cdots .$$

A significant point to be noted is that the recursive equation divided by dz gives the key estimate,

$$0 < r_{k-1}/d - x_k/z = r_k/(dz) < 1/z, \;\; k = 1, 2, \cdots .$$

This estimate represents a trivial fact: If a remainder is small in the division of n by d, then the next quotient is small. However, the result is not trivial at all. In practice the integer z is larger than 2^{30}, and $1/z$ is negligibly small as a bound. The inequality proves that each term in any sequence $\{u_k := x_k/z| \;\; k = 1, 2, \cdots, T\}$, which is to give uniform random number on a computer, is approximated as $v_k - 1/z < u_k < v_k$ within a small and uniform error bound $1/z \le 2^{-30}$ by the corresponding sequence

$$\{v_k := r_{k-1}/d| \;\; 0 < v_k < 1, \;\; r_{k-1} \equiv nz^{k-1} \bmod (d), \;\; k = 1, 2, \cdots, T\},$$

which is precisely the multiplicative congruential random number sequence generated by (d, z, n). As a mathematical principle, therefore, we need only to concentrate on finding a multiplicative congruential random number generator (d, z, n) of sufficiently long period T with good uniformity and independence. This transparent and firm perspective on the problem is further reinforced by spectral tests which are inseparably tied to multiplicative congruential generation of random numbers.

There have been two distinct types of choice in prior arts for the pair (d, z) of multiplicative congruential generator. One is formed by a large odd prime modulus $d = p$ with its primitive root multiplier z, and realizes the period $T = \varphi(p) = p - 1$, where φ is the Euler's function. The other

consists of a modulus $d = 2^i$ with $i \geq 4$ and any multiplier $z \equiv 5 \bmod (8)$ for the period $T = 2^{i-2}$. Both of these generators realize the largest period among all possible choices of multipliers for respective moduluses, and feasibly admit their respective spectral tests by plain mathematical principles, putting aside the resultant heavy computational burdens. Present inventions are direct descendants of the former, the pair of an odd prime modulus and its primitive root. Fishman and Moore (1986)[3] gave the monumental spectral tests on the Mersenne prime modulus $d = p = 2^{31} - 1$, and revealed the general and decisive fact that integers allow us to find a good generator (d, z) only by testing *all* primitive roots exhaustively, not at all admitting any hint that certain multipliers will be good or bad. This finding, however, disclosed a fundamental difficulty; the amount of computation increases in proportion to d^θ with the exponent $\theta \geq 3/2$ in *exhaustive* spectral tests. The test itself should be performed on the fastest computers of the time. And the computer requires its mounted random number generator to provide the largest number T of random numbers that can be consumed or computed in simulations of a month, say. This T should be the lower limit of the period that the random number generator (d, z) should have at any cost, but $T \leq d/2$ is a structural limitation of multiplicative congruential method. Thus, computers have the limit of computability proportional to d, but exhaustive spectral tests demand the total amount proportional to d^θ of computation with $\theta \geq 3/2$. This is the non-computability problem. Nakazawa and Nakazawa (2012a,b)[4] found that a breakthrough for this difficulty exists in the use of moduluses formed by products of two odd prime powers. Such constructions would reduce the computing time of exhaustive spectral tests to $O(d^\theta)$ with $\theta < 1$, while reserving the ratio of the period T to the modulus d to the value as large as the case of a pair of a prime and its primitive root. This is the design in which we look for the excellent generator (d, z, n) of uniform and independent random numbers.

3. Brief Summary of Inventions

Items **(i1)-(i3)** below outline the inventions to be presented. Though they refer to respective, distinct facet of the generation of uniform and independent random numbers, their integration will be seen to work strongly reinforcing each other.

(i1) A new, extended design of spectral tests as a strengthened sieve to extract a promising pair (d, z)

[3]Fishman and Moore (1986): G. S. Fishman and L. R. Moore, *An exhaustive analysis of multiplicative congruential random number generators with modulus* $2^{31} - 1$. SIAM Journal on Scientific and Statistical Computing, Vol. **7** (1986), pp. 24-45.

[4]Nakazawa and Nakazawa (2012a): N. Nakazawa and H. Nakazawa, *Computational progress in spectral tests of multiplicative congruential generators for uniform and independent random numbers realized by moduluses formed with two odd primes*. Filename *computable.pdf*, uploaded in http://www10.plala.or.jp/h-nkzw/ (October 26, 2012).
Nakazawa and Nakazawa (2012b): N. Nakazawa and H. Nakazawa, *Multiplicative congruential generators with moduluses formed by two odd-prime-factors for uniform and independent random numbers I. Computational analysis of structures*. Filename *revpopesq1.pdf*, uploaded in http://www10.plala.or.jp/h-nkzw/ (September 15-17, 2012, corrected on October 31, 2012).

of an odd modulus d and the multiplier z coprime to d as multiplicative congruential generator for uniform and independent random numbers with reliable statistical performance. Their resultant valuations should always be shown to consumers or users as the tag list for the generator (d, z) certifying its performances.

(i2) A new system of designs for the multiplicative congruential generator (d, z) comprising the modulus d and the multiplier z characterized by the following conditions **i2a)-i2e)**.

i2a) The modulus $d = d_1 d_2$ is a product of pairwise coprime factors d_1 and d_2 formed by two distinct odd primes p_1 and p_2 as $d_k = {p_k}^{i_k}$ for $k = 1, 2$ with indices $i_1 \geq 1$ and $i_2 \geq 1$.

i2b) Said odd prime p_1 has the form $p_1 = 2q + 1$ and said odd prime p_2 has the form $p_2 = 4r + 1$, with another odd primes q and r.

i2c) The multiplier z satisfies either one of the congruence relations $z \equiv z_1 \bmod (d_1)$ or $z \equiv -z_1 \bmod (d_1)$ for a primitive root z_1 of d_1.

i2d) The multiplier z satisfies the congruence relation $z \equiv z_2 \bmod (d_2)$ for a primitive root z_2 of d_2.

i2e) Noted odd primes p_1, p_2, q, r are all distinct.

(i3) Another new system of designs for the multiplicative congruential generator (d, z) comprising the modulus d and the multiplier z specified by the following conditions **i3a)-i3e)**.

i3a) the modulus $d = d_1 d_2$ is a product of pairwise coprime factors d_1 and d_2 formed by two distinct odd primes p_1 and p_2 as $d_k = {p_k}^{i_k}$ for $k = 1, 2$ with indices $i_1 \geq 1$ and $i_2 \geq 1$.

i3b) Said odd prime p_1 has the form $p_1 = 2q_1 + 1$ and said odd prime p_2 has the form $p_2 = 2q_2 + 1$ with another odd primes q_1 and q_2.

i3c) The multiplier z satisfies either the congruence relation $z \equiv z_1 \bmod (d_1)$ or the congruence relation $z \equiv -z_1 \bmod (d_1)$ for a primitive root z_1 of d_1.

i3d) The multiplier z satisfies either the congruence relation $z \equiv z_2 \bmod (d_2)$ or the congruence relation $z \equiv -z_2 \bmod (d_2)$ for a primitive root z_2 of d_2.

i3e) Noted odd primes p_1, p_2, q_1, q_2 are all distinct.

The use of the noted invention **(i2)** should be started by taking sufficiently many primitive root multipliers, z_1 of d_1 and z_2 of d_2, in said items **i2c)** and **i2d)**. They are recommended to be sieved in preparation by the extended spectral test of **(i1)**. Then, taking $\pm z_1$ and z_2 one after another, we need to use Sun Tzu's construction for the multiplier z by the system of congruence relations in **i2c)** and **i2d)**, to let (d, z) undergo **(i1)** as the second stage 2nd degree spectral test, and to let the passers undergo the final, higher degree spectral tests. The total passers, presumably very few if they do exist at all, are the brightest generators to be used on computers.

Likewise, the use of noted invention **(i3)** should be started by taking sufficiently many primitive root multipliers z_1 of d_1 and z_2 of d_2 in said items **i3c)** and **i3d)**. They are again recommended to be sieved in preparation by the extended spectral test of **(i1)**. Taking selected candidate $\pm z_1$ and $\pm z_2$ one after another, we use Sun Tzu's construction for the multiplier z by the system of congruence relations in **i3c)** and **i3d)**, let (d, z) undergo **(i1)** as the second stage 2nd degree spectral tests, and pick out the aimed generator for use on computers, if we could find excellent ones at all through higher degree spectral tests.

4. Detailed Description of the First Invention

4.1. Second Degree Spectral Tests

In order to expel ambiguities from descriptions, the sequence $\{n, nz, nz^2, \cdots\}$ from the multiplicative congruential generator (d, z, n) will first be taken as an infinite sequence without equivalence relations modulo d. Corresponding random numbers are reproduced as

$$v_1 = r_0/d, \;\; r_0 = n, \;\; 1 < r_0 < d,$$
$$v_k = r_{k-1}/d, \;\; r_k \equiv nz^k \bmod (d), \;\; 1 < r_k < d, \;\; k = 1, 2, \cdots .$$

We start with the 2nd degree spectral test taking consecutive 2-tuples from the generated sequence. Define the vector $\boldsymbol{Q}_k := (nz^{k-1}, nz^k) = nz^{k-1}(1, z)$; the vector $\boldsymbol{Q}_k$ is identified with the position vector of the point, and we call $\boldsymbol{Q}_k$ freely as the point itself. Let $\boldsymbol{Q}_k{}'$ denote any integer vector with coordinates equivalent to those of $\boldsymbol{Q}_k$ modulo d. Manifestly, $\boldsymbol{Q}_k{}'$ is obtained from the vector $\boldsymbol{Q}_k$ by some integral multiples of d translations along coordinate axes. Along the 2nd coordinate axis the d translation is effected by adding the vector $\boldsymbol{e}_2 := (0, d)$. And the d translation along the 1st axis is realized by adding

$$\boldsymbol{e}_1{}' := (d, 0) = d(1, z) - z(0, d) = d(1, z) - z\boldsymbol{e}_2.$$

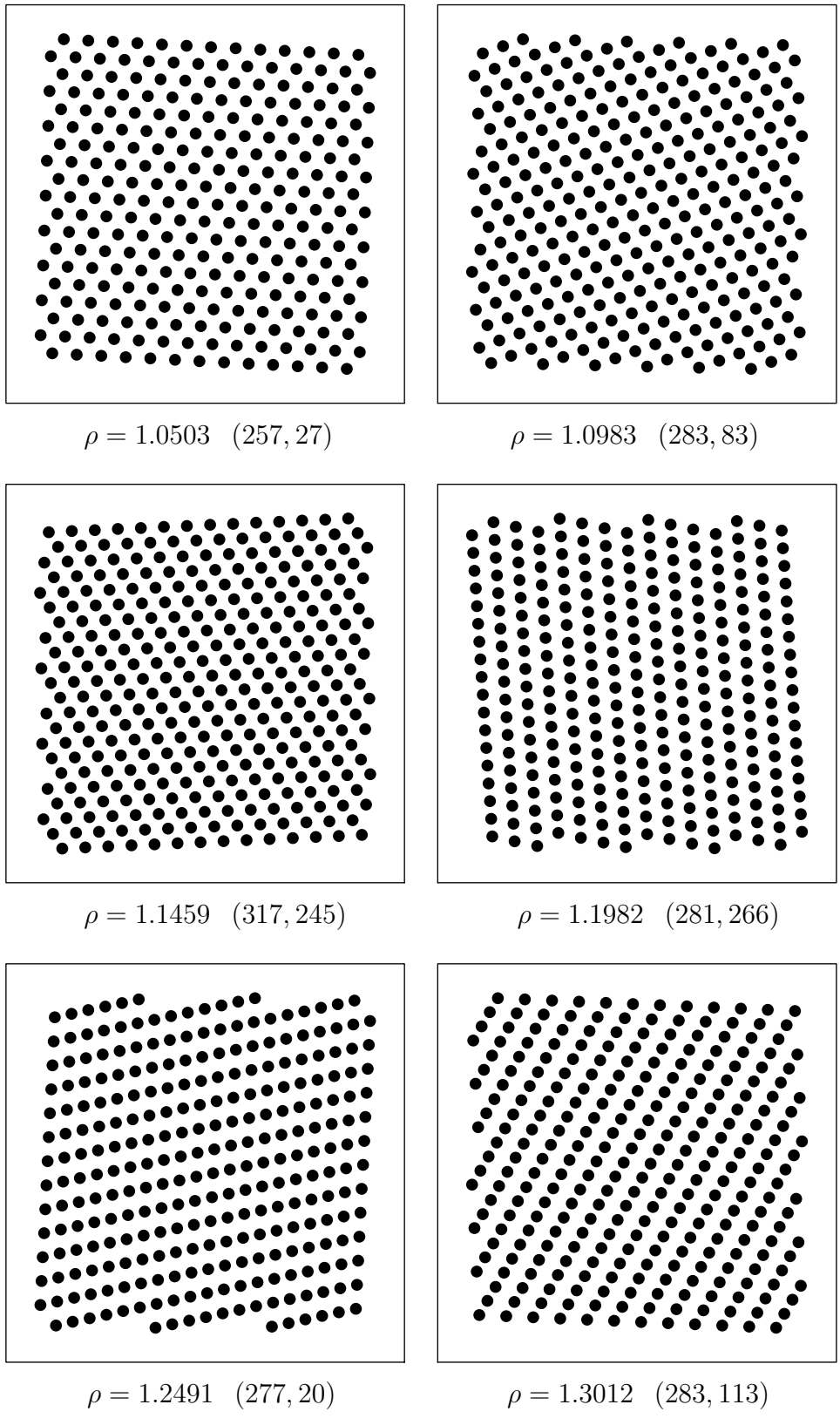
Therefore, every vector $\boldsymbol{Q}_k{}'$ with coordinates equivalent to $\boldsymbol{Q}_k$ modulo d is an integral linear combination of basis vectors

$$\boldsymbol{e}_1 := (1, z), \quad \boldsymbol{e}_2 := (0, d),$$

which are linearly independent in the sense that they give a non-zero determinant. All vectors or points with coordinates equivalent to those of $\boldsymbol{Q}_k$ are thus in the lattice spanned by basis vectors (or bases) $\{\boldsymbol{e}_1, \boldsymbol{e}_2\}$. We say points are *in* the lattice, because they cannot occupy the whole of lattice points. Typically, $\boldsymbol{Q}_k{}'$ cannot be any of points whose one or both of coordinates are equivalent to 0 modulo d. Let C_d denote the square in the Euclidean plane E_2 issuing from the origin with the interval $[0, d)$ as sides along axes. A significant fact is that this lattice is destined to have only d

lattice points in C_d. As a handy proof we may note that vectors $\{\boldsymbol{e}_1, \boldsymbol{e}_2\}$ span the area d by their

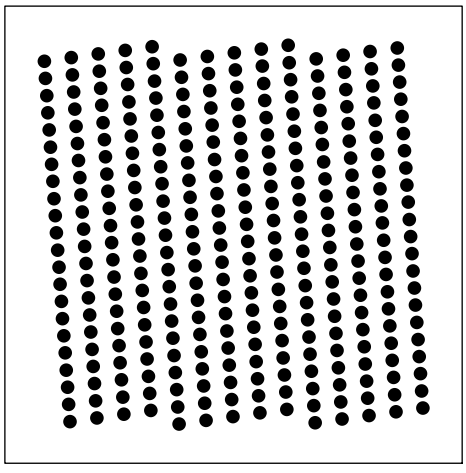
Figure 1 Geometry of 2-tuples of random numbers and spectral test valuation ρ



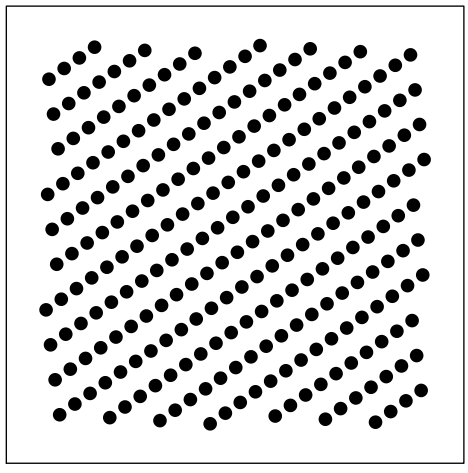
$\rho = 1.0503 \quad (257, 27)$ $\rho = 1.0983 \quad (283, 83)$

$\rho = 1.1459 \quad (317, 245)$ $\rho = 1.1982 \quad (281, 266)$

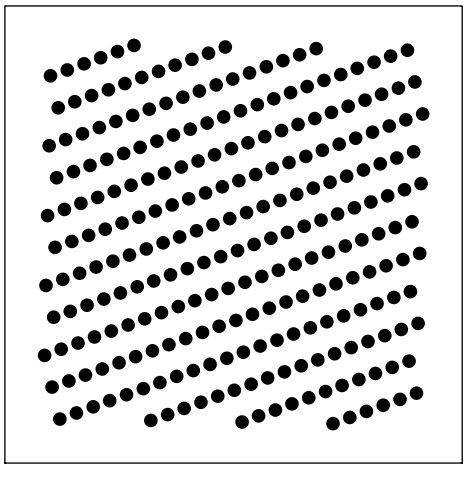
$\rho = 1.2491 \quad (277, 20)$ $\rho = 1.3012 \quad (283, 113)$



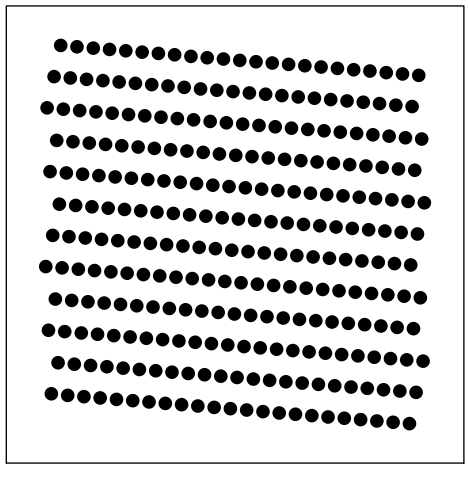
$\rho = 1.3501 \quad (311, 297)$



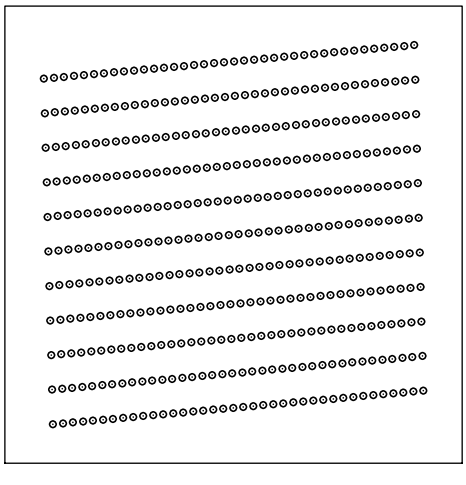
$\rho = 1.3947 \quad (251, 76)$



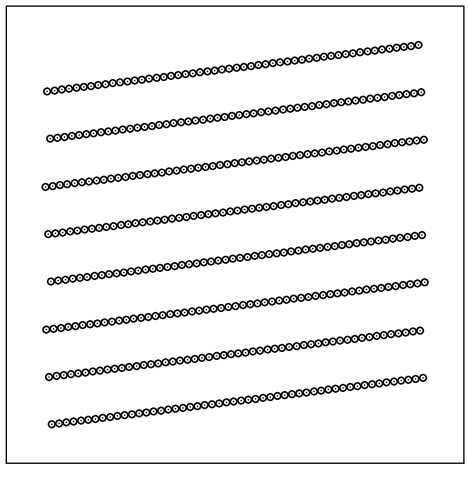
$\rho = 1.4547 \quad (251, 46)$



$\rho = 1.4959 \quad (281, 117)$



$\rho = 1.9915 \quad (419, 381)$



$\rho = 2.7283 \quad (419, 262)$

determinant, while the square C_d has the area d^2. More convincingly, a lattice vector

$$j\boldsymbol{e}_1 + k\boldsymbol{e}_2 = j(1, z) + k(0, d) = (j, jz + kd)$$

with integers j, k has the first component j which in C_d can take only $\{0, 1, \cdots, d-1\}$ as its d different values. Once j is fixed, the integer k has only one possible value so as for the second component $jz + kd$ to be in the interval $[0, d)$. The square C_d thus has exactly d lattice points. The generator (d, z, n) gives points $\{\boldsymbol{Q}_k\}$ in C_d whose modulo d equivalents are seated among these d lattice points. The rate of occupation of these d lattice seats can only be $(d-1)/d$ at the maximum.

The comprehension of noted facts is helped greatly by visual experiences. In the preceding two pages we showed plots of seats in the plane E_2 to be occupied by $(nz^{k-1}, nz^k) \bmod (d)$, consecutive 2-tuples from the generator (d, z) with a prime d and its primitive root z. The square depicted are taken slightly larger to include the square C_d of sides d issuing from the origin inside. Visual discernibility necessitates us to take small moduluses $d \approx 200$ with their suitable primitive roots z. Irrespective of these specific choices, plots show the general tendency. If z is not primitive, then plots should occupy only an integral fraction of these points by Lagrange's theorem. If the origin is supplemented, points will exhaust all of lattice points. The quantity $\rho := \rho_d^{(2)}(z) > 1$ is the valuation of the geometrical distribution of lattice points for respective generator (d, z). The definition of ρ will be given later. At this place it is only relevant to note that ρ closer to 1 from above implies that lattice points distribute more closely to the so-called triangular lattice. If $\rho \gg 1$ is the case, the configuration packs lattice points into fewer parallel lines (lattice lines) with large spacing between them. The spectral tests aims to find and pick out such a generator (d, z) with the valuation ρ closer to 1 from above. The historical criterion of Fishman and Moore (1986) was $\rho < 1.25$ for the passability of the generator (d, z).

4.2. The 1st Invention on the 2nd Degree Spectral Tests

Second degree spectral tests examine the geometry of the distribution of seats for points of two consecutive random numbers $(r_k, r_{k+1}) \equiv nz^{k-1}(1, z) \bmod (d)$. Just as the egg of Columbus, the problem is almost trivial if only we think of the geometrical distribution of points

$$(r_k, r_{k+l}) \equiv nz^{k-1}(1, z^l) \bmod (d), \quad l = 1, 2, 3, \cdots,$$

which for any $l = 2, 3, \cdots$ should be as good as the results for the generator (d, z) if the random numbers are truly uniform and independent. The geometry is examined easily by the 2nd degree spectral tests of the *multiplier* $z^l \bmod (d)$, or of the generator (d, z^l), *provided that this generator gives a long period comparable to that of the generator* (d, z). And, happy to say, 2nd degree spectral tests are easy to compute. Let us see what happens with the classical generators of Fishman and Moore (1986). Their **Table 2** lists top 5 primitive root multipliers for the Mersenne prime modulus $d = 2^{31} - 1 = 2147483647$ in the form of the row named **a)** in the following **Lists 2A-2E**.

The row named **1/a)** shows inverses of values in row **a)**, which correspond by definition to ρ-values[5]

List 2A $z = 742938285$

	2nd	**3rd**	**4th**	**5th**	**6th**
a)	0.8673	0.8607	0.8627	0.8320	0.8342
1/a)	1.1530	1.1618	1.1592	1.2019	1.1988
b)	1.15306751	1.16186656	1.15915450	1.20199716	1.19882541
	2nd of z^2	**2nd of z^3**	**2nd of z^4**	**2nd of z^5**	**2nd of z^6**
c)	1.91805599	1.81316446	1.32378868	3.25782855	1.04479227

List 2B $z = 950706376$

	2nd	**3rd**	**4th**	**5th**	**6th**
a)	0.8574	0.8985	0.8692	0.8337	0.8274
1/a)	1.1663	1.1130	1.1505	1.1995	1.2086
b)	1.16627569	1.11291561	1.15054146	1.19946130	1.20856552
	2nd of z^2	**2nd of z^3**	**2nd of z^4**	**2nd of z^5**	**2nd of z^6**
c)	1.19708825	6.76681886	1.46420589	5.00940631	2.26206864

List 2C $z = 1226874159$

	2nd	**3rd**	**4th**	**5th**	**6th**
a)	0.8411	0.8787	0.8255	0.8378	0.8441
1/a)	1.1889	1.1380	1.2114	1.1936	1.1847
b)	1.18893209	1.13803984	1.21140770	1.19360615	1.18426026
	2nd of z^2	**2nd of z^3**	**2nd of z^4**	**2nd of z^5**	**2nd of z^6**
c)	3.51885751	2.19846315	1.15368543	1.47158421	1.48916585

List 2D $z = 62089911$

	2nd	**3rd**	**4th**	**5th**	**6th**
a)	0.8930	0.8903	0.8575	0.8630	0.8249
1/a)	1.1198	1.1232	1.1662	1.1587	1.2123
b)	1.11986188	1.12320242	1.16615693	1.15876257	1.21227975
	2nd of z^2	**2nd of z^3**	**2nd of z^4**	**2nd of z^5**	**2nd of z^6**
c)	1.79072973	1.44118579	1.20332225	1.17058675	1.63022644

List 2E $z = 1343714483$

	2nd	**3rd**	**4th**	**5th**	**6th**
a)	0.8237	0.8324	0.8245	0.8262	0.8255
1/a)	1.2140	1.2013	1.2129	1.2104	1.2114
b)	1.21411121	1.20130010	1.21290241	1.21035116	1.21145141
	2nd of z^2	**2nd of z^3**	**2nd of z^4**	**2nd of z^5**	**2nd of z^6**
c)	1.99192650	1.45479150	1.13241226	1.56904222	1.04455900

[5]The numbers in the following lists were copied from the computer outputs and pasted. But inventors readily make mistypes and overlook fall out of numerals in revisions of manuscripts, and handling of manuscripts out from a patent office to another is liable to introduce complications further. Inventors express their deep regrets for their insufficient cares about all such errors, and ask readers to consider the circumstance and to rely on the following lists as the sufficiently proved originals.

listed in the row **b)**. The row **c)** gives the valuations of our present concern, valuations of the 2nd spectral test on (d, z^l) for $2 \leq l \leq 6$.

Computing processes to obtain these data are very easy, but results lead us to grave and significant recognitions. To be frank, we do not feel like using these listed multipliers or the generators (d, z) on our computers. More efficient use of the data from easily executable 2nd degree spectral tests of (d, z^l) generators for $l = 2, 3, \cdots$ should be made in finding and selecting an excellent generator (d, z) for our use in simulations. Admitting that this standpoint is approved, a significant question is: To how large an index l we should examine? At the present status of inventors' experiences the range $1 \leq l \leq 12$ seems to be the most adequate. Though we believe that passer generators (d, z^l) for $l \geq 13$ will exist in the 2nd degree spectral test, we could not find a passer within a reasonable magnitude of computing time. Since noted tests are only preparatory, they should give within available computing time sufficiently many passers to te tested further by 3rd to 6th degree spectral tests. In this respect 2nd tests for $1 \leq l \leq 12$ seem very fruitful and adequate. On the one hand they diminish candidates very efficiently within manageable time, and a few final passers of excellence could be found, again within a reasonable time. Of course, the final passers cannot be said abundant, but we strongly recommend to consult these 2nd tests as a standard mehod and indispensable device for the selection. We also recommend to post their results tagged on the generator as an able certificate of its excellence.[6]

5. The Second Invention

5.1. Preparations

From a more general point of view the facts listed in Tables 2A-2E show that the Mersenne prime modulus $d = p = 2^{31} - 1$ will not have a primitive root multiplier of satisfactory performance. We need to examine more odd primes, odd prime powers, or products of two such odd prime powers, and find good multiplicative congruential generators. The modulus $d = p = 2^{31} - 1$ is, above all, too small for computers of our day, and we should proceed to $d \approx 2^{48}$ or larger, say. We are thus confronted by difficulties of computability, and the possible way out is only to choose moduluses

[6] At this place we warn that spectral tests of degree $l \geq 3$ require revisions, and should be tried only with the next invention that will be accounted for later. It is not that the conventional spectral tests of such degrees, which aim to pick out the smallest value of *the largest distances between parallel adjacent lattice hyperplanes*, are in the wrong; all their procedures adopted up to the present invention from 1986 work correctly to their ends. The point is that they cannot realize the true aim of spectral tests, as realized and shown for the first time in the next invention of ours. It will be in order to note that excellent generators with two odd-prime-power moduluses were found *only with the use of said new inventions of ours*. Such successes are matters of course by the shuffling nature of the synthesis by Sun Tzus theorem, if subgenerators are to give excellent uniform and independent random number sequences. But conventional spectral tests have missed in selecting such (sub)generators of excellence in degrees $l \geq 3$. In this relation we also note that **List 2A** to **List 2E** in the preceding page present the non-revised 3rd to 6th results. Their revisions will be seen in the report to come with some notable consequences.

formed by two odd primes or two odd prime powers. Furthermore, we have to solve new problems arising with associated generators (d, z^2), (d, z^3), $\cdots$: Examine first their periods, and ask also on the existence or not of -1 in sequences they generate. Then perform at least 2nd degree tests of (d, z^2), (d, z^3), $\cdots$, so as to delete generators of little hope at the early stage of computation. Finally, go to 3rd to 6th spectral tests of outliving candidate generators.

Computational burdens should be diminished by any means. Happy to say, integers graciously allow us to note two new designs as particularly suited to alleviate some portions of these burdens. We concentrate here on preparations to facilitate the description of them. Two simple mathematical corollaries are the start. They suggest ways to select primes that have their primitive roots with orders consisting of small number of prime factor, and the knowledge will facilitate us to perform exhaustive spectral tests over relevant primitive roots.

Let an odd prime p be expressed as $p = 2q + 1$, and assume that the integer q is also an odd prime.[7] Examples $p = 7$ with $q = 3$ or $p = 23$ with $q = 11$ prove the existence of such prime pairs. In fact, computer experiments suggest their abundant, limitless existence. The following holds true.

Corollary 1. Let an odd prime $p \geq 7$ has the form $p = 2q + 1$ with another odd prime q. Then $2q - 2$ integers in $[2, p - 2 \equiv -2]$ form $q - 1$ pairs, each of which $(z, -z)$ consists of a primitive root z of the order $\varphi(p) = p - 1 = 2q$ and its negative $-z$ with the order q.

(Proof) The group $Z_p :\equiv \{1, 2, \cdots p - 1 = 2q\}$ modulo prime p is cyclic. Lagrange's theorem restricts the order of any element of Z_p to 1, 2, q or $2q$ for prime q. The equation $z^1 \equiv 1$ has the unique solution $z \equiv 1$, and $z \equiv \pm 1$ are all of solutions of $z^2 \equiv 1$. Any other $2q - 2$ integers have either q or $2q$ for their order. If the odd q is the order of z, then $(-z)^q \equiv -1$ holds and $-z$ is a primitive root. If z is a primitive root, $(-z)^q \equiv 1$ ensures $-z$ to have the order q. ■

The above corollary implies that $z = 2$ is either a primitive root or its negative modulo the noted special prime p. Thus, any relevant multiplier z modulo p may be expressed as a power of 2, and this fact helps and simplifies the execution of exhaustive spectral tests for such (p, z) generators.

Consider now an odd prime p of the form $p = 4r + 1$ with another odd prime r. Examples $p = 13$ or 29, and computer experiments convince us that such an odd prime p will exist without limit.

Corollary 2. If an odd prime $p \geq 13$ has the form $p = 4r + 1$ with another odd prime r, then $z = 2$ is a primitive root of p.

(Proof) Direct computations of the power of 2 for $p = 13$ show that 2 is a primitive root modulo 13. We therefore assume $p \geq 29$, $r \geq 7$. The group of integers coprime to p consists of $\varphi(p) = 4r$ equivalence classes, and Lagrange's theorem stipulates that the order of $z = 2$ is a factor of $4r$,

[7] This type of prime q was used by Sophie Germain in her classic contribution to Fermat's last theorem. See Harold M. Edwards: *Fermat's Last Theorem* in *Graduate Texts in Mathematics 50*, Springer (1977).

which are exhausted by $\{1, 2, 4, r, 2r, 4r\}$. The assumption $p \geq 29$ proves that the order of $z = 2$ is not $1, 2, 4$. We prove that $z^{2r} \equiv -1 \bmod (p)$; this proves that z^r is not equivalent to 1 modulo p, so that the order of $z = 2$ is $4r$ and full. The product

$$M := (2 \cdot 1)(2 \cdot 2) \cdots (2 \cdot r) \cdot \{2 \cdot (r+1)\}\{2 \cdot (r+2)\} \cdots \{2 \cdot (2r)\} = 2^{2r}(2r)!$$

has another expression modulo p:

$$\begin{aligned} M &= 2 \cdot 4 \cdots (2r) \cdot (2r+2) \cdot (2r+4) \cdots (2r+2r) \\ &= 2 \cdot 4 \cdots (2r) \cdots \{p-(2r-1)\} \cdot \{p-(2r-3)\} \cdots (p-1) \\ &\equiv (-1)^r (2r)! = -(2r)! \bmod (p). \end{aligned}$$

Note that r is odd. We thus have $2^{2r}(2r)! \equiv -(2r)! \bmod (p)$, or $2^{2r} \equiv -1 \bmod (p)$ because $(2r)!$ is coprime to the odd prime $p = 4r + 1$. ■

This proof was communicated to Hiroshi Nakazawa by Naoya Nakazawa on April 17, 2013. Just as Corollary 1, this comprehension is helpful for exhaustive spectral tests of (p, z).

Computations with noted corollaries at once suggest the following:

Conjecture 3. If an odd prime $p \geq 7$ has the form $p = 2q + 1$ with another odd prime q, then for any integral exponent $i \geq 1$ the multiplier $z = 2$ either is a primitive root of $d = p^i$ with the order $\varphi(p^i) = 2qp^{i-1} = 2qd/p$, or is the negative of a primitive root with $qp^{i-1} = qd/p$ for its half-full order. **(End of Conjecture 3)**

Conjecture 4. If an odd prime $p \geq 13$ has the form $p = 4r + 1$ with another odd prime r, then for any integral exponent $i \geq 1$ the multiplier $z = 2$ has the full order $\varphi(p^i) = 4rp^{i-1} = 4rd/p$ and is a primitive root of $d = p^i$. **(End of Conjecture 4)**

These Conjectures are true if only they could be shown for the case $i = 2$, but we could not arrive at the proof. Yet, computers prove that they are true up to $p < 10^7 = 2^{23.25}$; they might well be imagined true and, if we need some modulus of the form p^i, we may readily let computers confirm the conjecture with $z = 2$ at the start.

Stated Corollaries and Conjectures suggest us to start the design of multiplicative congruential generators using odd primes of noted types. Besides the said facilities that they give $\varphi(p^i)$ with small numbers of prime factors and simplify ways to sweep over their primitive roots, we shall find in this way more of structural advantages, related to the necessity for us to consider generators of the type (d, z^j) with $j \geq 2$, by giving them simpler structures of periods.

5.2. Further Preparations to Describe Second and Third Inventions

For proofs on the 2nd and the 3rd inventions, it will be advisable to summarize necessary notions further. Computations to come are all performed on the stage of moduluses formed by two odd

prime powers, and involve two main players, pairs of primitive roots for respective odd prime powers that construct multipliers by Sun Tzu's construction from systems of congruence relations. Our concern is to compute periods realized by noted arrangements, and also to answer the question whether -1 arises or not in generated sequences.

Arguments will be helped greatly by the following corollaries.

Corollary 5. Let d_1, d_2 be mutually coprime integers, and let z_k be a multiplier coprime to d_k for $k = 1, 2$. Assume that the generator (d_k, z_k) has the order or the period T_k, and they are synthesized into the generator (d, z) defined by

$$d := d_1 d_2, \quad z :\equiv z_k \bmod (d_k), \quad k = 1, 2.$$

The cyclic sequence, generated from (d, z) and now defined as $G(z; d) :\equiv \{1, z, z^2, \cdots\} \bmod (d)$, has the order or the period T as the least common multiple, $T := \mathrm{LCM}(T_1, T_2)$.

(Proof) At this occasion we refer to Sun Tzu's construction associated with his theorem that gives the solution z of noted system of congruence relations modulo d. Since d_1 and d_2 are coprime with $\mathrm{GCD}(d_1, d_2) = 1$, Euclidean algorithm gives integers A, B satisfying $Ad_1 + Bd_2 = 1$. Integers $U_1 := Bd_2 = 1 - Ad_1$ and $U_2 := Ad_1 = 1 - Bd_2$ are determined by d_1 and d_2 alone without dependence on z_1 or z_2, and satisfy $U_j \bmod (d_k) = \delta_{jk}$. Therefore, a solution z of noted system of congruence relations is

$$z \equiv z_1 U_1 + z_2 U_2 \bmod (d).$$

Any other solution z' gives $z - z' \equiv 0 \bmod (d_k)$ for both of $k = 1, 2$, so that $z - z'$ is divisible by coprime d_1 as well as d_2, or by $d = d_1 d_2 = \mathrm{LCM}(d_1, d_2)$. Hence $z' \equiv z \bmod (d)$ holds true as the uniqueness modulo d. Direct computations of z^j or the observation $z^j \equiv (z_k)^j \bmod (d_k)$ for $k = 1, 2$ at once prove

$$z^j \equiv (z_1)^j U_1 + (z_2)^j U_2 \bmod (d), \quad j = 1, 2, \cdots.$$

Increasing j up to T, we have

$$1 \equiv z^T \equiv (z_1)^T U_1 + (z_2)^T U_2 \bmod (d),$$

for which $(z_k)^T \equiv 1 \bmod (d_k)$ should hold true for $k = 1, 2$. Therefore, the order or the period of $G(z; d)$ is the least common multiple of T_1 and T_2 ■

The statement below will be obvious.

Corollary 6. Assume that the generator (d, z) or its cyclic sequence $G(z; d)$ has the period or the order T. The generator (d, z^j) or the cyclic sequence $G(z^j; d)$ realizes the period

$$T^{(j)} := T/\mathrm{GCD}(j, T)$$

for any power index $j = 1, 2, \cdots$. **(End of Corollary 6)**

We may note several summaries that will help discussions on the appearance or not of -1 in the cyclic sequence $G(z^j; d)$ of the generator (d, z^j), in particular for z defined by congruence relations $z \equiv z_k \bmod (d_k)$ for $k = 1, 2$ with coprime d_1 and d_2.

Corollary 7. **(A1)** If the cyclic sequence $G(z; d)$ does not include $-1 \bmod (d)$, then cyclic sequences $G(z^j; d)$ for any index $j = 1, 2, \cdots$ are free from -1 modulo d.

(A2) Resume the notation $T^{(j)}$ for the order or the period of the cyclic sequence $G(z^j; d)$ with any $j = 1, 2, \cdots$. In order for $G(z^j; d)$ to include $-1 \bmod (d)$, the period $T^{(j)}$ is necessarily even. The contraposition is: If $T^{(j)}$ is odd, the cyclic sequence $G(z^j; d)$ does not include -1 modulo d.

(B) If the modulus $d = d_1 d_2$ is a product of two coprime factors d_1 and d_2, and z is defined by $z \equiv z_k \bmod (d_k)$ for $k = 1, 2$, then following statements **(B1)** and **(B2)** hold true on the appearance or not of -1 in the cyclic sequence $G(z^j; d)$.

(B1) If at least one of component cyclic sequences $G(z_k; d_k)$ for $k = 1$ or 2 is devoid of -1 modulo d_k, then the cyclic sequence $G(z^j; d)$ for any index $j = 1, 2, \cdots$ is free from -1 modulo d.

(B2) Let the modulus $d = d_1 d_2$ be composite, and the index $j \geq 1$ be arbitrary. An even period $T^{(j)}$ of the cyclic sequence $G(z^j; d)$ is not always sufficient for the appearance of -1 modulo d in $G(z^j; d)$. A necessary and sufficient condition for the appearance of -1 modulo d in $G(z^j; d)$ is that $T^{(j)}$ is even *and* both of cyclic subsequences $\{G((z_k)^j; d_k) |\ \ k = 1, 2\}$ have -1 modulo d_k *in tune* at $T^{(j)}/2$, i.e. there hold $\{(z_k)^j\}^{T^{(j)}/2} \equiv -1 \bmod (d_k)$ for both of $k = 1$ and 2.

(Proof) **(A1)** The assertion is obvious, because the cyclic group $G(z^j; d)$ for any $j = 2, 3, \cdots$ is a subgroup contained in the larger reduced residue class group $G(z; d)$ of integers modulo d.

(A2) If the cyclic sequence $G(z^j; d)$ has $-1 \equiv d - 1 \bmod (d)$ at $0 < T' < T^{(j)}$, then we have $(z^j)^{T'} \equiv -1 \bmod (d)$, $(z^j)^{2T'} \equiv 1 \bmod (d)$. Thus, $0 < 2T' < 2T^{(j)}$ is a multiple of $T^{(j)}$, and $2T' = T^{(j)}$ holds true. Hence $T^{(j)}$ is necessarily even with $T' = T^{(j)}/2$.

(B1) If the cyclic sequence $G(z; d)$ has $-1 \equiv d - 1 \bmod (d)$, then $G(z_k; d_k) \equiv G(z; d) \bmod (d_k)$ contains $-1 \bmod (d_k)$ for both of $k = 1, 2$. The contraposition proves the assertion.

(B2) We shall soon see an example of the cyclic sequence $G(z^j; d)$ with an even $T^{(j)}$ but without -1. We prove the necessary and sufficient part. If -1 is in the cyclic sequence $G(z^j; d)$, then $T^{(j)}$ is even by **(A2)**, and also $(z^j)^{T^{(j)}/2} \equiv -1 \bmod (d)$ is true by the proof of **(A2)**. Therefore, we have relations

$$(z^j)^{T^{(j)}/2} \equiv \{(z_k)^j\}^{T^{(j)}/2} \equiv -1 \bmod (d_k), \quad k = 1, 2,$$

which is the necessary part of **(B2)**. Suppose conversely that $T^{(j)}$ is even and congruence relations

$$(z^j)^{T^{(j)}/2} \equiv -1 \bmod (d_k), \quad k = 1, 2,$$

hold true. These are the system of congruence relations,

$$(z^j)^{T^{(j)}/2} \equiv \{(z_k)^j\}^{T^{(j)}/2} \equiv -1 \bmod (d_k), \quad k = 1, 2,$$

and $(z^j)^{T^{(j)}/2} \equiv -1 \bmod (d)$ is manifestly their modulo d unique solution. Hence the sufficient part of **(B2)** follows. ■

6. Second and Third Inventions

6.1. The Second Invention

We are now able to describe with ease two inventions on structurally advantageous designs of multiplicative congruential generator (d, z). One of them takes the construction of (d, z) fulfilling 7 conditions **(2a)-(2g)** listed below.

(2a) The modulus d is a product of two coprime factors $d = d_1 d_2$, where d_1 and d_2 will be called submoduluses.

(2b) The submodulus $d_1 = (p_1)^{i_1}$ is a power of an odd prime p_1 with an integral index $i_1 \geq 1$ and the odd prime p_1 has the form $p_1 = 2q + 1$ with another odd prime q.

(2c) The submodulus $d_2 = (p_2)^{i_2}$ is a power of an odd prime p_2 with an integral index $i_2 \geq 1$ and the odd prime p_2 has the form $p_2 = 4r + 1$ with another odd prime r.

(2d) Odd primes p_1, p_2, q, r are all distinct.

(2e) The multiplier z is defined by the system of congruence equations,

$$z \equiv z_k \bmod (d_k), \quad k = 1, 2,$$

where z_1 and z_2 will be called submultipliers.

(2f) The submultiplier z_1 is either a primitive root, or the negative of a primitive root, of the submodulus d_1.

(2g) The submultiplier z_2 is a primitive root of the submodulus d_2.

These constitute the 2nd invention to be described. Performances of the generator (d, z^j) designed by these specifications **(2a)-(2g)** are posted in the next page as **List 3A** and **List 3B**. Emphases are here on the quantity which we name the ***efficiency*** of the generator (d, z^j) for respective $j = 1, 2, \cdots$ and symbolize as τ:

$$\text{(efficiency)} := \tau := \{\text{usable period of } (d, z^j)\}/d.$$

The first **List 3A** refers to the choice of the submultiplier z_1 that is a primitive root of the submodulus $d_1 = (p_1)^{i_1}$. The generator (d_1, z_1) will be called the subgenerator. By assumption z_1 has the largest order T_1 modulo d_1,

$$T_1 := \varphi(d_1) = \{(p_1)^{i_1 - 1}\}(p_1 - 1) = 2qd_1/p_1.$$

List 3A z_1 is a primitive root of d_1 with the order $2qd_1/p_1$,
z_2 is a primitive root of d_2 with the order $4rd_2/p_2$.

z^j	The LCM order of $z' := z^j$ modulo d	Is the cyclic sequence of z' inclusive of -1?	Approximate τ
z	$4qrd_1d_2/(p_1p_2)$	no	$1/2$
z^2	$2qrd_1d_2/(p_1p_2)$	no	$1/4$
z^3	$4qrd_1d_2/(p_1p_2)$	no	$1/2$
z^4	$qrd_1d_2/(p_1p_2)$	no	$1/8$
z^5	$4qrd_1d_2/(p_1p_2)$	no	$1/2$
z^6	$2qrd_1d_2/(p_1p_2)$	no	$1/4$
z^7	$4qrd_1d_2/(p_1p_2)$	no	$1/2$
z^8	$qrd_1d_2/(p_1p_2)$	no	$1/8$

List 3B z_1 is the negative of a primitive root of d_1 with the order qd_1/p_1,
z_2 is a primitive root of d_2 with the order $4rd_2/p_2$.

z^j	The LCM order of $z' := z^j$ modulo d	Is the cyclic sequence of z' inclusive of -1?	Approximate τ
z	$4qrd_1d_2/(p_1p_2)$	no	$1/2$
z^2	$2qrd_1d_2/(p_1p_2)$	no	$1/4$
z^3	$4qrd_1d_2/(p_1p_2)$	no	$1/2$
z^4	$qrd_1d_2/(p_1p_2)$	no	$1/8$
z^5	$4qrd_1d_2/(p_1p_2)$	no	$1/2$
z^6	$2qrd_1d_2/(p_1p_2)$	no	$1/4$
z^7	$4qrd_1d_2/(p_1p_2)$	no	$1/2$
z^8	$qrd_1d_2/(p_1p_2)$	no	$1/8$

The subgenerator (d_2, z_2) has the primitive root z_2 of the submodulus d_2, and gives the largest order T_2 modulo d_2,

$$T_2 := \varphi(d_2) = \{(p_2)^{i_2-1}\}(p_2 - 1) = 4rd_2/p_2.$$

The generator $(d = d_1d_2, z)$ is defined by the system of congruence relations specified in **(2e)**, and **Corollary 5** ensures the synthesized (d, z) to have the least common multiple order or period T,

$$T := \mathrm{LCM}(T_1, T_2) = \mathrm{LCM}(2qd_1/p_1, 4rd_2/p_2) = 4qrd/(p_1p_2).$$

The order of (d, z^j) may now be computed by **Corollary 6** for any $j = 1, 2, 3, \cdots$ as

$$T^{(j)} := \{\text{the period of } G(z_j; d)\} = T/\mathrm{GCD}(j, T) = T/\mathrm{GCD}(j, 4qrd/(p_1p_2)).$$

The formula gives three meaningful cases, by the assumed **(2a)-(2d)**:

(2A1) If $j < \min(q, r)$ is odd, then the order $T^{(j)} = T$.

(2A2) If $j < \min(q, r)$ is even but not a multiple of 4, then $T^{(j)} = T/2$.

(2A3) If $j < \min(q, r)$ is a multiple of 4, then $T^{(j)} = T/4$.

We should turn next to examine whether -1 arises or not in the cyclic sequence $G(z^j; d)$ and find the usable period, to be denoted ${T_u}^{(j)}$, of $G(z^j; d)$ in the use as independent random numbers. We should creep through the situation that submultipliers z_1, z_2 are primitive roots and necessary itinerate respective -1 in their cyclic sequences. We therefore resort to **(B2)** and **(A1)** of **Corollary 7** and show the *detuning*, in the technological terminology, due to $G(z_1; d_1)$. From $T = 4qrd/(p_1p_2)$ and putting $T/2 = T_1N$ with an integer N, we have

$$(z_1)^{T/2} = \{(z_1)^{T_1}\}^N \equiv 1 \bmod (d_1).$$

Thus, -1 does not arise in $G(z; d)$, and **(A1)** of **Corollary 7** ensures $G(z^j; d)$ to be devoid of -1 for any index $j < \min(q, r)$. Thus ${T_u}^{(j)} = T^{(j)}$ holds, and all orders or periods of cyclic sequences in **List 3A** are usable. We conclude the following for the efficiency τ.

(2A1) For rows with odd j: $\tau = T/d \approx 1/2$.

(2A2) For rows of even j not divisible by 4: $\tau = (T/2)/d \approx 1/4$.

(2A3) For rows with j divisible by 4: $\tau = (T/4)/d \approx 1/8$.

These complete the proof of **List 3A**.

Consider now the remaining case that the submultiplier for the submodulus d_1 in the design **(2f)** is a negative of a primitive root. We denote the submultiplier as $-z_1$ implying that z_1 is a primitive root modulo d_1. The primitive root z_1 generates the cyclic sequence

$$\{1, z_1, (z_1)^2, \cdots, (z_1)^{T_1/2} \equiv -1, \cdots, (z_1)^{T_1} \equiv 1\} \bmod (d_1)$$

with length $T_1 = 2qd_1/p_1$ consisting of all integers distinct modulo d_1. In particular, integers in the first half of the sequence $\{1, z_1, (z_1)^2, \cdots, (z_1)^{T_1/2-1}\}$ are not equivalent to ± 1 modulo d_1, so that the fact that $T_1/2 = qd_1/p_1$ is odd gives that $(-z_1)^{T_1/2} \equiv 1 \bmod (d_1)$ occurs for the first time in the sequence $\{-z_1, (-z_1)^2, \cdots\}$. Thus, the order or the period of the cyclic sequence $G(-z_1; d_1)$ is $T_1/2$ and odd, and $-z_1$ is not a primitive root modulo d_1. Yet **Corollary 6** ensures that the order or the period of $G(z; d)$ is

$$\text{(the order of } z \text{ modulo } d) = \mathrm{LCM}(T_1/2, T_2) = \mathrm{LCM}(qd_1/p_1, 4rd_2/p_2) = 4qrd/(p_1p_2).$$

This is identical with the case of the primitive root submultiplier, and all resulting orders of z^j for $j < \min(q, r)$ are the same likewise. And the odd order of $-z_1$ stipulates that the cyclic subsequence $G(-z_1; d_1)$ is devoid of -1. Thus **(A2)** of **Corollary 7** proves that all of **List 3B** are concerned with the case ${T_u}^{(j)} = T^{(j)}$, and the efficiencies in **List 3B** remains identical with those of **List 3A**.

6.2. The Third Invention

In the second invention noted above, the efficiency $\tau =$ (usable period)/d of the generator (d, z^j) for $j \leq \min(q, r)$ varies from $1/2$ to $1/8$. This is a tame fluctuation, particularly in contrast to cases of the modulus $d = 2^i$ to be elucidated later. In practice we shall choose a large enough d and cut the nominal period of the generator (d, z) down to $d/8$ with little problem. Yet, the variation of usable periods of $z, z^2, \cdots$ might be felt a little conspicuous. After all it is unknown whether naturally and beautifully flat usable periods of $(d, z), (d, z^2), \cdots$ will contribute so as for more multipliers to have better performances. Yet our intuition tempts us, whispering that a more flat and even usable periods in variations of j might be better or might give more abundantly *excellent* multipliers. Heavy loads of computation are in our front as spectral test search for a generator (d, z) with reliable statistics, and we would like to exploit *any* devices that might lessen the toil and give successes. The following specific form of the modulus realizes the flatness at a small expense of diminishing the largest value of the efficiencies. It will be worth noting that inventors' systematic efforts with time consuming computation to find excellent generators have so far been fruitful only in this design. Though available resources and time of inventors are too limited to claim for the outstanding generality of this circumstance, we recommend the design as advantageous with some reliable assurances.

The relevant generator design is characterized by 7 conditions **(3a)** to **(3g)** listed below.

(3a) The modulus d is a product of two coporime factors $d = d_1 d_2$, where d_1 and d_2 will again be called submoduluses.

(3b) The submodulus $d_1 = (p_1)^{i_1}$ is a power of an odd prime p_1 to an integral index $i_1 \geq 1$, where p_1 has the form $p_1 = 2q_1 + 1$ with another odd prime q_1.

(3c) The submodulus $d_2 = (p_2)^{i_2}$ is a power of an odd prime p_2 to an integral index $i_2 \geq 1$, where p_2 has the form $p_2 = 2q_2 + 1$ with another odd prime q_2.

(3d) Odd primes p_1, p_2, q_1, q_2 are all distinct.

(3e) The multiplier z is defined by the system of congruential equations,

$$z \equiv z_k \bmod (d_k), \quad k = 1, 2,$$

where z_1 and z_2 will be called submultipliers.

(3f) The submultiplier z_1 is either a primitive root, or the negative of a primitive root, of the submodulus d_1.

(3g) The submultiplier z_2 is either a primitive root, or the negative of a primitive root, of the submodulus d_2.

Resultant performances of the generator (d, z) are summarized in **List 4A** to **List 4C** below. We

prove them one by one, showing the merit of noted designs.

List 4A For both of $k = 1$ and 2 z_k is primitive modulo d_k with the order $2q_kd_k/p_k$

z^j	The LCM order of $z' := z^j$ modulo d	Is the cyclic sequence of z' inclusive of -1?	Approximate τ
z	$2q_1q_2d_1d_2/(p_1p_2)$	yes	$1/4$
z^2	$q_1q_2d_1d_2/(p_1p_2)$	no	$1/4$
z^3	$2q_1q_2d_1d_2/(p_1p_2)$	yes	$1/4$
z^4	$q_1q_2d_1d_2/(p_1p_2)$	no	$1/4$
z^5	$2q_1q_2d_1d_2/(p_1p_2)$	yes	$1/4$
z^6	$q_1q_2d_1d_2/(p_1p_2)$	no	$1/4$
z^7	$2q_1q_2d_1d_2/(p_1p_2)$	yes	$1/4$
z^8	$q_1q_2d_1d_2/(p_1p_2)$	no	$1/4$

List 4B Case of a primitive root and a negative of primitive root

z^j	The LCM order of $z' := z^j$ modulo d	Is the cyclic sequence of z' inclusive of -1?	Approximate τ
z	$2q_1q_2d_1d_2/(p_1p_2)$	no	$1/2$
z^2	$q_1q_2d_1d_2/(p_1p_2)$	no	$1/4$
z^3	$2q_1q_2d_1d_2/(p_1p_2)$	no	$1/2$
z^4	$q_1q_2d_1d_2/(p_1p_2)$	no	$1/4$
z^5	$2q_1q_2d_1d_2/(p_1p_2)$	no	$1/2$
z^6	$q_1q_2d_1d_2/(p_1p_2)$	no	$1/4$
z^7	$2q_1q_2d_1d_2/(p_1p_2)$	no	$1/2$
z^8	$q_1q_2d_1d_2/(p_1p_2)$	no	$1/4$

List 4C Both of multipliers are negatives of primitive roots

z^j	The LCM order of $z' := z^j$ modulo d	Is the cyclic sequence of z' inclusive of -1?	Approximate τ
z	$q_1q_2d_1d_2/(p_1p_2)$	no	$1/4$
z^2	$q_1q_2d_1d_2/(p_1p_2)$	no	$1/4$
z^3	$q_1q_2d_1d_2/(p_1p_2)$	no	$1/4$
z^4	$q_1q_2d_1d_2/(p_1p_2)$	no	$1/4$
z^5	$q_1q_2d_1d_2/(p_1p_2)$	no	$1/4$
z^6	$q_1q_2d_1d_2/(p_1p_2)$	no	$1/4$
z^7	$q_1q_2d_1d_2/(p_1p_2)$	no	$1/4$
z^8	$q_1q_2d_1d_2/(p_1p_2)$	no	$1/4$

First, **List 4A** takes primitive root submultipliers z_1 and z_2 in **(3f)** and **(3g)**. Subgenerators (d_k, z_k) for $k = 1, 2$ have even orders

$$T_k := \varphi(d_k) = (p_k)^{i_k-1}(p_k - 1) = 2q_kd_k/p_k, \quad k = 1, 2,$$

and realize $(z_k)^{T_k/2} \equiv -1 \bmod (d_k)$ in their midways. Also, **Corollary 5** proves the order T of $G(z;d)$ as

$$T := \mathrm{LCM}(T_1, T_2) = \mathrm{LCM}(2q_1d_1/p_1, 2q_2d_2/p_2) = 2q_1q_2d/(p_1p_2).$$

The order $T^{(j)}$, with j taken among one of $1, 2, \cdots$, of the cyclic sequence $G(z^j;d)$ is now classified into two kinds **(3Ao)** and **(3Ae)** by **Corollary 6**:

(3Ao) Case of odd $j < \min(q_1, q_2)$: $T^{(j)} = T = T_1(T_2/2) = (T_1/2)T_2 = (\mathrm{even})$,

(3Ae) Case of even $j < \min(q_1, q_2)$: $T^{(j)} = T/2 = q_1q_2d/(p_1p_2) = (\mathrm{odd})$.

Thus, an even j gives an odd $T^{(j)}$, and the cyclic sequence $G(z^j;d)$ does not include -1 by **(A2)** of **Corollary 7**. There holds ${T_u}^{(j)} = T^{(j)}$, and we have the proof of even j rows of **List 4A**:

$$(\text{the efficiency } \tau \text{ for any even } j) = T^{(j)}/d \approx 1/4.$$

In contrast an odd j gives an even $T^{(j)}$. We need $\{(z_k)^j\}^{T^{(j)}/2} \bmod (d_k)$ to be examined for both of $k = 1, 2$, with $T^{(j)}/2 = T/2 = (T_1/2)(T_2/2)$ now beng a product of odd integers. This implies

$$\begin{aligned}\{(z_k)^j\}^{T/2} &= \{[(z_k)^j]^{T_k/2}\}^{(\text{an odd integer})} \\ &= \{(z_k)^{T_k/2}\}^{j\times(\text{an odd integer})} \\ &\equiv (-1)^{(\text{an odd integer})} \equiv -1 \bmod (d_k),\end{aligned}$$

irrespective of $k = 1, 2$. For $z' := (z_k)^j$ with an odd j, we thus have that cyclic subsequences

$$G((z')^m; d_k) \equiv \{(z')^{m-1} \bmod (d_k) |\ \ m = 1, 2, \cdots\}$$

for $k = 1, 2$ are both equivalent *in tune* to $-1 \bmod (d_k)$ at $m = T/2$. By **(B2)** of **Corollary 7** there holds $(z^j)^{T/2} \equiv -1 \bmod (d)$. The usable period is ${T_u}^{(j)} = T^{(j)}/2 = T/2$ for $G(z^j;d)$, and the efficiency is $\tau = (T/2)/d \approx 1/4$. Proofs of odd j rows or the whole of **List 4A** is completed.

Consider now the case that one of submultipliers, which we take without loss of generality to be the first and denote $-z_1$, is the negative of a primitive root z_1 of d_1, while the other is the primitive root z_2 of d_2. Results of this case shown in **List 4B** are to be proved. The cyclic subsequence $G(-z_1;d_1)$ has the order ${T_1}' := T_1/2 = q_1d_1/p_1$ which is odd. Therefore, **(A2)** of **Corollary 7** approves that $G(z^j;d)$ is devoid of -1 for any $j = 1, 2, \cdots$ and the whole of orders of $G(z^j;d)$ is usable. The order of $G(z;d)$ is

$$(\text{the order of z}) = \mathrm{LCM}({T_1}', T_2) = \mathrm{LCM}(q_1d_1/p_1, 2q_2d_2/p_2) = 2q_1q_2d/(p_1p_2) = T.$$

This is identical with the order T of the preceding case **List 4A** that both of submultipliers are primitive roots. Hence all cyclic sequences $G(z^j;d)$ for integral index $j < \min(q_1, q_2)$ have the identical orders as before. Analyses prove the orders $T^{(j)}$ as follows;

odd $j < \min(q_1, q_2)$: $T^{(j)} = T = T_1(T_2/2) = (T_1/2)T_2$,
even $j < \min(q_1, q_2)$: $T^{(j)} = T/2 = (T_1/2)(T_2/2)$.

The difference to the preceding case of **List 4A** is that, irrespective of whether j is even or odd, the whole of these orders are usable by the absence of -1. The efficiencies are thus concluded as

$$\text{odd}j : \tau = T/d \approx 1/2, \quad \text{even } j : \tau = (T/2)/d \approx 1/4,$$

which are all to be proved for **List 4B**.

Take finally the third case that both of submultipliers are negatives, $-z_1$ and $-z_2$, of primitive roots. Subgenerators $(d_1, -z_1)$ and $(d_2, -z_2)$ have respective orders $T_1{}'$ and $T_2{}'$:

$$T_1{}' = T_1/2 = q_1 d_1/p_1, \quad T_2{}' = T_2/2 = q_2 d_2/p_2.$$

The period T' of the synthesized cyclic sequence $G(z; d)$ is given by

$$T' := \mathrm{LCM}(T_1{}', T_2{}') = \mathrm{LCM}(q_1 d_1/p_1, q_2 d_2/p_2) = q_1 q_2 d/(p_1 p_2) = T/2.$$

This is odd. The cyclic sequence $G(z^j; d)$ with $j < \min(q_1, q_2)$ has one and the the same odd order $T'/\mathrm{GCD}(j, T') = T'$. From this, or by any of **(A1)**, **(A2)** or **(B1)** of **Corollary 7**, all relevant generators lack -1 in their cyclic sequences, and the efficiency τ is unified to

$$\tau = T'/d = q_1 q_2/(p_1 p_2) \approx 1/4.$$

These prove all of **List 4C**. ■

7. Actual Procedures of Invented Second Degree Spectral Tests

Before the closing, we present some subtle details arising in problems of spectral tests. We limit arguments to the realization of inventions 1-3, namely to the 2nd degree spectral tests. This limitation is somewhat inappropriate deplorably, but we put a greater importance to the visibility of the geometry of the Euclidean plane E_2.

Consecutive 2-tuples of points $\{(nz^k, nz^{k+1}) = nz^k(1, z) |\ \ k = 0, 1, 2, \cdots\}$ and their modulo d equivalents emitted from the generator (d, z) were seen in Sec. 4 to be in a lattice $G := G(\boldsymbol{e}_1, \boldsymbol{e}_2)$ spanned by basis vectors $\{\boldsymbol{e}_1 = (1, z), \boldsymbol{e}_2 = (0, d)\}$. We take a slight generalization, and consider a lattice $G' := G'(\boldsymbol{e}_1{}', \boldsymbol{e}_2{}')$ spanned by basis vectors $\{\boldsymbol{e}_1{}', \boldsymbol{e}_2{}'\}$ in the Euclidean plane E_2 by their integral linear combinations,

$$G' = G'(\boldsymbol{e}_1{}', \boldsymbol{e}_2{}') = \{c_1 \boldsymbol{e}_1{}' + c_2 \boldsymbol{e}_2{}' |\ \ (c_1, c_2 \text{ are integers})\}.$$

Readers are referred to any plot in **Figure 1** as the visual image of such a lattice.

We first note a general way to take the basis vectors on a given lattice G'. Let an arbitrary lattice point be P. Draw a line L', to be called a *lattice line*, connecting P to any other lattice point Q. Among infinite number of lattice points on L', points P, Q are assumed to be neighboring. Draw other lattice line L'' which is parallel and neighboring to L' without any other parallel lattice lines in between. Choose an arbitrary lattice point R on L''. Then vectors

$$\boldsymbol{e}_1{}' := \overrightarrow{PQ}, \quad \boldsymbol{e}_2{}' := \overrightarrow{PR}$$

are a set of basis vectors of the lattice G':

Corollary 8. Any vectors $\{\boldsymbol{e}_1{}', \boldsymbol{e}_2{}'\}$ constructed by the noted way are basis vectors of an arbitrary lattice G' in E_2. They span a parallelogram of one and the same area. Any set of basis vectors of G' are linear transformations of others by unimodular integer matrices.[8]

(Proof) We may translate the parallelogram, formed by vectors $\{\boldsymbol{e}_1{}', \boldsymbol{e}_2{}'\}$ constructed in noted procedures, along its two sides (lattice lines), let its one vertex P itinerate every lattice point of G', and let its area tile the plane E_2 completely without any opening or overlap. Therefore, $\{\boldsymbol{e}_1{}', \boldsymbol{e}_2{}'\}$ is a set of basis vectors of the lattice G'. The same performance is realized by any choice of different basis vectors $\{\boldsymbol{e}_1{}'', \boldsymbol{e}_2{}''\}$ with a different shape constructed in the noted way, if their parallelogram has the same area associated with every lattice point. All set of basis vectors of G' are constructed in this way, and the way exhausts the choice of basis vectors of G'. Any other basis vectors $\{\boldsymbol{e}_1{}'', \boldsymbol{e}_2{}''\}$ are integral linear combinations of $\{\boldsymbol{e}_1{}', \boldsymbol{e}_2{}'\}$, so that the matrix M'' formed by $\{\boldsymbol{e}_1{}'', \boldsymbol{e}_2{}''\}$ has the relation $M'' = M'U$ to the matrix M' formed by $\{\boldsymbol{e}_1{}', \boldsymbol{e}_2{}'\}$ by a matrix U with integer components. Since determinants of both sides should agree except for the sign, we have $\det U = \pm 1$, namely U should be a unimodular matrix with a unimodular inverse. ■

We now have the perspective of general circumstances.

Corollary 9. Let there be given an arbitrary lattice $G' = G'(\boldsymbol{e}_1{}', \boldsymbol{e}_2{}')$ in the Euclidean plane E_2. Name the triangle spanned by any set of basis vectors $\{\boldsymbol{e}_1{}', \boldsymbol{e}_2{}'\}$ as a *2-simplex*. Denote $\overline{\lambda}'$ for the largest distance between parallel neighboring lattice lines in G'. There holds

$$\overline{\lambda}' = \sup_{\text{all 2-simplexes of } G'} \text{(the largest vertex height from the base line in a 2-simplex)}.$$

(Proof) By the construction of basis vectors of a lattice G', the distance λ' of any set of parallel neighboring lattice lines is the height of a vertex P of some 2-simplex to the baseline facing P. Conversely, any height of any vertex in an arbitrary 2-simplex is the distance of some neighboring parallel lattice lines. Therefore, λ' is given as the supremum over all 2-simplexes in G'. ■

[8] A square martix U is unimodular if U consists of integers components and if $\det U = \pm 1$ holds true. Then inverse matrix U^{-1} is also unimodular, manifestly.

We now have:

Corollary 10. As to the distribution of points of the lattice $G = G(\boldsymbol{e}_1, \boldsymbol{e}_2)$ for the 2nd degree spectral tests of the (d, z) there hold the following.

(A) The ideal geometrical form of the lattice G, for the statistical inference that the generator (d, z) gives uniform and independent random numbers, is given by the triangular lattice constructed with regular 2-simplexes with the largest distance $\overline{\lambda}_d^{(2)} := 2^{1/2}3^{-1/4}d^{1/2}$ between parallel and neighboring lattice lines.

(B) The lattice $G = G(\boldsymbol{e}_1, \boldsymbol{e}_2)$, that provides seats to 2-tuples of random numbers emitted from (d, z), has the largest distance $\lambda = \lambda_d^{(2)}(z)$ between its parallel and neighboring lattice lines, with λ bounded from below as follows:

$$\lambda = \lambda_d^{(2)}(z) > \overline{\lambda}_d^{(2)} = 2^{1/2}3^{-1/4}d^{1/2} \approx 1.07456993d^{1/2}.$$

(Proof) **(A)** The configuration of seats as a triangular lattice certainly give least reasons to negate the statistical hypothesis that consecutive 2-tuples from the generator do not have the uniformity or the independence. Drawing pictures of a regular triangle of the area $d/2$, we at once have the value of $\overline{\lambda}_d^{(2)}$ with the trigonometric calculus, say.

(B) Take a triangle of a fixed area $d/2$ and its any edge with length a. Let the edge face the vertex with the height h. By $ah = d$, the shortest edge corresponds to the largest height h in the triangle. If the triangle is not regular, its shortest edge length a should satisfy $a < \overline{a}$ for the edge length $\overline{a}$ of the regular triangle. Thus, $h = d/a \geq d/\overline{a} =: \overline{h}$ holds true for the height $\overline{h} = \overline{\lambda}_d^{(2)}$ of the regular triangle by **(A)**. Since the lattice $G(\boldsymbol{e}_1, \boldsymbol{e}_2)$ cannot have irrational coordinates for its lattice points, the equality never arises. ■

In order to perform actual computations of 2nd degree spectral tests, we had better be transferred to the dual lattice. We discuss with general lattices.

Corollary 11. Take the lattice $G' = G'(\boldsymbol{e}_1{}', \boldsymbol{e}_2{}')$ in E_2 defined by any set of linearly independent basis vectors $\{\boldsymbol{e}_1{}', \boldsymbol{e}_2{}'\}$. Define the dual basis vectors $\boldsymbol{f}_1{}', \boldsymbol{f}_2{}'$ by inner products

$$(\boldsymbol{e}_j{}', \boldsymbol{f}_k{}') = \delta_{jk}.$$

Name the lattice spanned by dual basis vectors $\{\boldsymbol{f}_1{}', \boldsymbol{f}_2{}'\}$ as the dual lattice G'^* of G', with its any set of (dual) basis vectors being constructed operationally in the same way as in G'. Any set of basis vectors $\{\boldsymbol{e}_1{}', \boldsymbol{e}_2{}'\}$ of G' corresponds to a unique set of dual basis vectors $\{\boldsymbol{f}_1{}', \boldsymbol{f}_2{}'\}$ of G'^*, and conversely any set of dual basis vectors $\{\boldsymbol{f}_1{}', \boldsymbol{f}_2{}'\}$ of G'^* corresponds to a unique set of basis vectors $\{\boldsymbol{e}_1{}', \boldsymbol{e}_2{}'\}$ of G'.

(Proof) Denote by M' the 2×2 matrix formed by row vectors $\boldsymbol{e}_1{}', \boldsymbol{e}_2{}'$. The set of inner products is identical with the matrix equation $M'^{\,t}\{(M')^*\} = I$, where $(M')^*$ is the 2×2 matrix formed by row

vectors $\boldsymbol{f}_1{}', \boldsymbol{f}_2{}'$, the matrix ${}^t\{(M')^*\}$ is the transpose of $(M')^*$, and I is the 2×2 unit matrix. Therefore, $(M')^*$ is well-defined and unique once M' is given. Their correspondence is manifestly invertible, as well as one-to-one and onto:

$$M'^* = {}^t\{(M')^{-1}\}, \quad M' = {}^t\{(M'^*)^{-1}\}. \qquad \blacksquare$$

The aim of this subsection is to state the following relation.

Theorem 12. Take any lattice G' in E_2 defined by any given set of linearly independent basis vectors $\{\boldsymbol{e}_1{}', \boldsymbol{e}_2{}'\}$. Denote λ for the largest distance of the two neighboring lattice lines in G'. This largest distance is given by the smallest, non-zero vector $\boldsymbol{f}_{\min}{}'$ of the dual lattice as

$$\lambda = 1/\|\boldsymbol{f}_{\min}{}'\|,$$

where $\|\boldsymbol{f}_{\min}{}'\|$ is the Euclidean length of $\boldsymbol{f}_{\min}{}'$.

(Proof) Let any 2-simplex of the lattice G' in E_2 be denoted as the triangle $\triangle PQR$. The choice of names of vertices is irrelevant, so that we take Q facing the base line $\overline{RP}$ and evaluate the height λ' of Q. We may choose $\boldsymbol{e}_1{}' := \overrightarrow{PQ}$ and $\boldsymbol{e}_2{}' := \overrightarrow{PR}$ as the basis vectors and define the dual basis vectors $\boldsymbol{f}_1{}', \boldsymbol{f}_2{}'$ which are determined uniquely by basis vectors. Since $\boldsymbol{f}_1{}'$ is orthogonal to the base line $\boldsymbol{e}_2{}' = -\overrightarrow{RP}$, the height is given as

$$\lambda' = |(\boldsymbol{e}_1{}', \boldsymbol{f}_1{}')|/\|\boldsymbol{f}_1{}'\| = 1/\|\boldsymbol{f}_1{}'\|.$$

The smallest of this value over all set of *basis* vectors is the same as the smallest taken over all dual vectors, and the proof is complete. $\blacksquare$

Theorem 12 transposes the search for the largest spacing of parallel adjacent lattice lines in E_2 to the search of the shortest non-zero vector of dual lattice. To this latter end it is advisable to first represent dual lattice vectors by integers only; this enables us to execute the work in the error-free integer arithmetic for any length of computing time. This is at once in spectral tests. Corresponding to the basis vectors $\boldsymbol{e}_1 = (1, z)$ and $\boldsymbol{e}_2 = (0, d)$, we may define:

$$\boldsymbol{f}_1 = (d, 0), \quad \boldsymbol{f}_2 = (-z, 1).$$

The following inner products are obviou:

$$(\boldsymbol{e}_j, \boldsymbol{f}_k) = d\delta_{jk}, \quad 1 \leq j, k \leq 2.$$

These are readily assembled into **Theorem 12.** Let F^* denote the 2×2 matrix formed by these integer row vectors $\{\boldsymbol{f}_1, \boldsymbol{f}_2\}$. Inner product relations are the same as follows:

$$M\,{}^tF^* = dI, \quad F^* = d\,{}^tM^{-1} = dM^*.$$

Therefore, we have $\boldsymbol{f}_j{}' = \boldsymbol{f}_j/d$ for $j = 1, 2$, and

$$\lambda = d/\|\boldsymbol{f}_{\min}\|,$$

with the integer shortest vector $\boldsymbol{f}_{\min}$ in the dual lattice $G^* := G(\boldsymbol{f}_1, \boldsymbol{f}_2)$.

Now that the problem is reduced to the search of the shortest integer dual lattice vector $\boldsymbol{f}_{\min}$ in the dual lattice, we may profitably take dual vectors in *cartesian* coordinates $\boldsymbol{f} = (j_1, j_2)$ with integers j_1, j_2. We have:

Corollary 13. The necessary and sufficient condition, for the integer vector $\boldsymbol{f} = (j_1, j_2)$ to be in the 2-dimensional dual lattice G^* of the (d, z) generator, is the following:

$$j_1 + zj_2 \equiv 0 \bmod (d).$$

(Proof) If $\boldsymbol{f} = (j_1, j_2)$ is in the dual lattice G^*, integers m_1, m_2 exist and give $\boldsymbol{f} = m_1\boldsymbol{f}_1 + m_2\boldsymbol{f}_2$ or $j_1 = dm_1 - zm_2$ and $j_2 = m_2$. Therefore, $j_1 + zj_2 = dm_1 \equiv 0 \bmod (d)$ holds true and the condition is necessary. Conversely, if the condition is satisfied, an integer k exists and gives $j_1 + zj_2 = kd$, or

$$\boldsymbol{f} = (j_1, j_2) = (kd - zj_2, j_2) = k\boldsymbol{f}_1 + j_2\boldsymbol{f}_2.$$

Thus $\boldsymbol{f}$ is in the dual lattice G^*, and the condition is also sufficient. ■

There is a final clue for the 2nd degree spectral tests that facilitates the search of the shortest dual lattice vector $\boldsymbol{f}_{\min}$ in E_2. Namely, the length of this shortest vector has a geometrical upper bound.

Corollary 14. The largest distance $\lambda_d^{(2)}(z)$ of the parallel, adjacent lattice lines in the lattice in E_2 given by the generator (d, z) has the geometrical lower bound $\overline{\lambda}_d^{(2)}$,

$$\lambda_d^{(2)}(z) = d/\|\boldsymbol{f}_{\min}\| > \overline{\lambda}_d^{(2)} := 2^{-1/2}3^{1/4}d^{-1/2},$$

which equivalently implies that the shortest dual lattice vector $\boldsymbol{f}_{\min}$ of the (d, z) generator has the following geometrical upper bound:

$$\|\boldsymbol{f}_{\min}\| < 2^{1/2}3^{-1/4}d^{1/2} \approx 1.07456993d^{1/2}.$$

(Proof) We prove directly the more exotic upper bound of $\|\boldsymbol{f}_{\min}\|$. Triangles or 2-simplexes spanned by lattice basis vectors have one and the same area $d/2$. Any dual basis vectors also span a lattice named dual lattice, so that by the relation of matrices M and F (or by an explicit form of F) F should also span the parallelogram of area d, or the 2-simplex of area $d/2$. Under this restriction of a fixed area $d/2$ triangles can have the smallest edge that should not exceed the case of a regular triangle, $\|\boldsymbol{f}_{\min}\| \leq 2^{1/2}3^{-1/4}d^{1/2}$. Since a regular triangle of area $d/2$ necessarily have irrational

coordinates, the 2-simplexes of the dual lattice cannot reproduce the equality in this relation by their integral coordinates. ■

Existence of this geometrical restriction is an evidence that (2nd degree) spectral tests of (d, z) are not too much vicious as a shortest vector problem. Let $\lambda_d^{(2)}(z)$ denote the largest distance λ of parallel, adjacent lattice lines in the lattice spanned by 2-tuples emitted from the (d, z) generator. The aim of the 2nd degree spectral tests is to find (d, z) such that the following valuation,

$$\rho = \rho_d^{(2)}(z) := \lambda_d^{(2)}(z)/\overline{\lambda}_d^{(2)} = d/(\|\boldsymbol{f}_{\min}\|\overline{\lambda}_d^{(2)}) = 2^{1/2}3^{-1/4}d^{1/2}/\|\boldsymbol{f}_{\min}\|,$$

is not much apart from the lower limit 1, even though ρ is destined to be larger than 1. The passability criterion of (d, z) is usually taken as $\rho < 1.25$ after Fishman and Moore (1986). We are now able to explain how to carry out this second degree tests. First, give candidates for modulus d and multiplier z. Then fix the desired range of ρ, usually $1 < \rho < 1.25$. Let the integer j_2 sweep in the range $|j_2| < 2^{1/2}3^{-1/4}d^{1/2}$, compute $j_1 \equiv -zj_2 \bmod (d)$, and evaluate

$$2^{1/2}3^{-1/4}d^{1/2}/\{{j_1}^2 + {j_2}^2\}^{1/2}.$$

The smallest value of this quantity is the 2nd degree valuation $\rho_d^{(2)}(z)$ of the generator (d, z). We should repeat tests taking different multiplier z and different modulus d until we find a generator with satisfactory performance. We need the strategy, the conviction and the patience.

In the passing, we would like to add the following. All geometrical arguments noted above work beautifully and we are completely in the right, thanks to the accidentally simple circumstance of 2-dimensional geometry. However, by implications of spectral tests, the way of geometrical thinking in higher dimension requires revisions from a different standpoint. This will be discussed fully in accounting the next invention. There we shall see some seemingly small revisions will reward us with impressive technological successes in the accurate generation of uniform and independent random numbers.

8. Two Concluding Remarks

8.1. Computational Procedures with Moduluses Formed by Two Odd-Prime-Factors

Any design of a multiplicative congruential generator (d, z) starts from the choice of the modulus d. Putting aside the overview provided by the arithmetic structure, that any finite sequence of uniformly bound integers may be approximated by a multiplicative congruential sequence, we were motivated strongly by the conviction of the utility of shuffling structures in Sun Tzu's theorem. The simple-minded first direction was to look for generators with the largest efficiency

$$\tau := (\text{the usable period } T')/d \approx 1/2.$$

More recent realization of ours, that 2nd degree spectral test performances of generators (d, z^k) for $k \geq 2$ are vital, reformed us to look into securing flat structures of periods for these constructed generators. The 2nd and the 3rd inventions are now believed to be the most adequate structures to this end. But we do not have resources to chase after two hares. Up to the present we have been working only with the 3rd invention of the modulus d constructed as

$$d = p_1 p_2, \quad p_1 = 2q_1 + 1, \quad p_2 = 2q_2 + 1,$$

with distinct odd primes p_1, q_1, p_2, q_2. Our guess is that the form $d = {p_1}^{i_1} {p_2}^{i_2}$ with indices $i_1, i_2 \geq 1$, as well as the 2nd invention with the modulus

$$d = {p_1}^{i_1} {p_2}^{i_2}, \quad p_1 = 2q + 1, \quad p_2 = 4r + 1.$$

with distinct odd primes p_1, q, p_2, r, will likewise be fruitful candidates. Yet, we cannot have general perspectives or good results for all of these. We therefore concentrate on the special case of the 3rd invention with the simple product $d = p_1 p_2$ and primes q_1, q_2 for $p_k = 2q_k + 1,\ k = 1, 2$.

The merit and the advantage of this design will be accounted for most clearly by describing the explicit procedures adopted in successful search processes.

(1) Fix the starting prime p_1 and the final prime $\overline{p}_1$, and design the computation so as to proceed by increasing p_2 to $p_2 + 2$ step by step up to $\overline{p}_1$, checking that p_1, q_1, p_2, q_2 are primes.

(2) For a $d_1 = p_1$ take 2 as the smallest primitive root or its negative, and proceed on the 2nd spectral test of (p_1, z^k) with k increased consecutively as $k = 1, 3, 5, \cdots$, say up to $k = 12$.

(3) Proceed similarly with $d_2 = p_2$.

(4) We then take two lists of passers, a passer (p_1, z_1) and a passer (p_2, z_2), combine them by Sun Tzu's theorem to a generator $(d = p_1 p_2, z)$ and perform its 2nd stage spectral tests, namely 2nd degree tests of (d, z^k) for $k = 1, 2, \cdots, 6$ and 3rd to 6th tests of (d, z), say.

We have no computing time to try on $d = {p_1}^{i_1} {p_2}^{i_2}$, and the circumstances are completely open to our knowledge. There may be devised different ways to prepare passers (p_1, z_1) and (p_2, z_2); for example we may perform spectral tests of 3rd to 6th degrees on (p_1, z_1) to lessen the passers, and likewise for (p_2, z_2). This is in a sense dangerous as tactics, because there may be and in fact there were synthesized passers whose component subgenerators did not pass their respective 3rd to 6th degree spectral tests. But the diminished number of candidates may give a shorter time in finding a good passer. Many devices, conspiracies and arts will be needed to avoid unnecessary computations, but with care.

Readers are asked not to undertake these procedures at this place. This is because spectral tests of 3rd to 6th degrees require revisions, without which the success will be hard to be attained. The

subject will be accounted for fully in the next report on the 2nd invention now under submission to Patent Offices of Nations.

8.2. Moduluses Including Powers of 2

The design of the modulus d with two odd prime factors was seen to have various excellent features. Its merits may be grasped in engineering terms as realizing the shuffling of two subgenerators which, as a machine with two motors with respective periods, can be designed to realize *detuning* that expels dangerous resonance and, with excellently polished submotors, may realize a smoother and excellent total system. Above all, the design will be the sole way to get rid of problems of computability and to equip contemporary fast computers with *tested* generators of sufficiently long periods.

Multiplicative congruential generators for uniform and independent random numbers have another influential design that adopts the power of the prime 2 as the modulus, $d = 2^i$. A simple condition $z \equiv 5 \bmod (8)$ ensures the largest possible period $T = 2^{i-2} = d/4$ in this case, and the whole of this T is usable by the absence of -1 in the sequence if only the initial value n is chosen so as to satisfy $n \equiv 1$ or $5 \bmod (8)$.[9] In an epoch making work Fishman (1990)[10] conducted spectral tests adopting the modulus $d = 2^{32}$ and exhausting all possible multipliers $z \equiv 5 \bmod (8)$. He also presented examinations of a portion of multipliers for $d = 2^{48}$; computational difficulties prevented him to perform exhaustive tests in the latter case. Thus, from the start the modulus $d = 2^i$ has carried difficult problems of computability. Nakazawa and Nakazawa (2008)[11] showed that the problem cannot be resolved by taking composite moduluses in this case. If a power of 2 enters a modulus d as a factor in the product with odd primes or odd-prime-powers, it inevitably introduces correlations among powers of submultipliers for odd primes, and the resultant random numbers cannot be taken as independent. This flaw is vicious in the sense that it cannot be detected by spectral tests. Stated differently, the modulus $d = 2^i$ should be used standing alone if at all, for any multiplicative congruential generator and severe difficulties of computation in exhaustive spectral tests have no way to be alleviated from the status met in Fishman (1990). We note here another problem with this type of moduluses.

Suppose we have a generator (d, z) with $d = 2^i$ and $z \equiv 5 \bmod (8)$. We saw that (d, z^k) for $k = 2, 3, \cdots$ should also be good random number generators. However, difficulties seem to arise

[9] This is because $5^j \equiv 1$ or $5 \equiv -3 \bmod (8)$ holds true for any $j = 1, 2, \cdots$.

[10] Fishman (1990): G. S. Fishman, *Multiplicative congruential random number generators with modulus 2^β: An exhaustive analysis for $\beta = 32$ and a partial analysis for $\beta = 48$.* Mathematics of Computation, Vol. **54** (1990), pp.331-344.

[11] Nakazawa and Nakazawa (2008): H. Nakazawa and N. Nakazawa, *Designs of uniform and independent random numbers with long period and high precision — Control of the sequential geometry through product group structures and lattice configurations.* Filename *3978erv.pdf*, uploaded in http://www10.plala.or.jp/h-nkzw/ (March 9-July 8, 2008).

with their orders, for example. Since the generator ($d = 2^i, z$) has the order $T = 2^{i-2}$, the generator (d, z^k) has the order

$$T' = T/\mathrm{GCD}(k, T) = T/\mathrm{GCD}(k, 2^{i-2}).$$

If the exponent k of the multiplier reaches $k = 2^m$ for $m < i - 2$, a sudden change of the period to $T' = T/2^m$ arises, though this shorter-period sequence is wholly usable by the absence of -1 with any multiplier $z \equiv 5 \bmod (8)$. This feature looks to be unfit for generators $(d = 2^i, z^k)$ with various index k to realize evenly excellent independence as random numbers. But this is only a guess harbored in a frightened mind that is unwilling to set out to very heavy computations of spectral tests with uncertain prospects. The true performance of generators should be confirmed with numerical reality, of course.