Note: Revisit to the Mersenne Prime Modulus of Fishman and Moore

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

(September 13, 2015)

A recent revisit to the historical Marsenne prime modulus $d = p = 2^{31} - 1 = 2147483647$ of Fishman and Moore (1986)[2] disclosed interesting and suggestive insights on random number problems. This note is hoped to be helpful in sharing this significant overview with engineers as well as users needing random numbers in various fields. We denote a multiplicative congruential generator based on the modulus d and the multiplier z as (d, z). The modulus $d \geq 2$ may be any integer not necessarily a prime, and the multiplier z may be any integer only demanded to be coprime to d. Full devices and adequate specifications will be needed, of course, in order to realize long periods with excellent statistics of generated random numbe sequences.

Regarding spectral tests of (d, z) generators, Nakazawa and Nakazawa (2013)[3] found powerful roles of *2nd degree tests* of generators (d, z^k) for $k = 2, 3, \cdots$, in the examination of the original (d, z) random number sequence with a particular attention on the sequential correlation between pairs emitted with k steps apart. These spectral tests were advocated for use as powerful techniques to select excellent (d, z) random number sequences with excellent statistical independence.

By some will of the Goddess of Fortune, the discovery was followed by another finding that spectral tests with degrees larger than 2 require a new system of criteria based on the lattice geometry with *regular simplex* forms of their unit cells. See Nakazawa and Nakazawa (2014a, 2015).[4] It is well recognized that the technology is now confronted by needs for

[1]nmail@nakazawa-patents.jp

[2]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.

[3]Filed for Patent Applications in 2013. See Nakazawa and Nakazawa (2014): Naoya Nakazawa and Hiroshi Nakazawa, *Constructive design of uniform and independent random number generators*, uploaded in *http://nakazawa-patents.jp* with the filename *invention1a.pdf* on April 29-August 5, 2014.

[4]Nakazawa and Nakazawa (2014a): Naoya Nakazawa and Hiroshi Nakazawa, *Methods of spectral tests of multiplicative congruentialrandom number generators*, uploaded in *http://nakazawa-patents.jp* on June 5, 2014 with the filename *invention 2k.pdf* / Nakazawa and Nakazawa (2015): Naoya Nakazawa and Hiroshi Nakazawa, *The geometry of spectral tests, ibid.*, uploaded with the filename *sptest15june7naorev.pdf* on March 20-June 7, 2015.

random number sequences with both of large periods and *tested* excellent statistics, so as to lead large scale simulations requiring large moduluses, say $d \geq 2^{52}$. To our pleasure the problem has been solved in a somewhat old invention of Nakazawa and Nakazawa (2008)[5] that moduluses formed by two odd primes can reduce the spectral test computation to a tractable amount. In fact, Nakazawa and Nakazawa have obtained[6] nearly a dozen of (d, z) generators with excellent spectral test valuations and with the period T not less than 2^{50} in this method.

We are happy with all these results, which were obtained in a hurried computation without enjoying stages on which respective integers are playing their roles. However, the desired periods of random number sequence will increase without limit in the advent of faster computers, and we should continue our efforts to find random number sequences with still better performances and still larger periods. A question thus occurred to us: Can we say with confidence that we know well about the behavior of integers so as to extend our successful expeditions for excellent sets of integers filling such requests? We cannot help feeling that the answer is no. This short report aims to convey the feeling which was intensified by results obtained very recenly in a specific analysis of the Mersenne prime modulus $d = p = 2^{31} - 1 = 2147483647$ taken in the work Fishman and Moore (1986).[2] This prime modulus $d = p$ was convicted erroneously by the present authors to be fruitless by the finding that generators reported by Fishman and Moore failed the extended 2nd degree spectral tests of (p, z^k) for $2 \leq k \leq 6$ in a rather disappointing manner. As noted, this finding was *before* the other finding that spectral tests with degrees greater than 2 should be altered, by some malicious or gracious will of the Goddess of Fortune. The Inventors are reminded of a question: What will be the matter, if primitive roots of this prime modulus is tested exhaustively *both* by extended 2nd tests of (p, z^k) for $k = 1, 2, 3, \cdots$ *and* by revised 3rd to 6th degree spectral tests of (p, z)?

Happy to say, our desktop computers are very fast these days. They enable us to execute the noted exhaustive search for excellent primitive root multipliers in no more than 3 days.[7] Results were quite suggestive.[8] We note here the *top* primitive root forming a pair $\{z, z^{-1}\}$

[5]Nakazawa and Nakazawa (2008): Hiroshi Nakazawa and Naoya Nakazawa. *Designs of uniform and independent random numbers with long periods and high precision*, uploaded in *http://www10.plala.or.jp/h-nkzw/pastreports.html* on March 9-July 8, 2008 with the filename *3978erv.pdf*.

[6]See *Prospectus of Nakazawa Patents*, posted in *http://nakazawa-patents.jp* with the filename *eprospectus141026.pdf* on July 12-October 26, 2014.

[7]If we let m "command prompts" work simultaneously on a computer with each carrying a program with m-divided range of data, then the total computing time will be reduced to $1/m$, say for $m \approx 4$. But we were not so hasty in the noted computation.

[8]We post the program $fishmanmoorenao.for$ and its output *fishmanmoorenao.txt* by Naoya Nakazawa and Hiroshi Nakazawa in a downloadable form in the present URL. Readers are invited to make its free private

modulo p with the same valuation, and the second best primitive root among all primitive roots of $p = 2^{31} - 1$. We shall also note a suggestive example of good-looking z which nevertheless let us reflect on how we should design the construction of spectral tests.

The star multiplier at the top is $z = 318320879 \equiv 7^{69539149} \ (\mathrm{mod} p)$ with $p = 2^{31} - 1$. This is the representative of the pair $\{z, z^{-1}\}$ of the same valuation[9] with $z^{-1} \equiv 447299545 \equiv 7^{2077944497} \ (\mathrm{mod} p)$.[10] Splendid valuations of this multiplier z are shown below.

$\rho_p^{(2)}(z)$	$\rho_p^{(2)}(z^2)$	$\rho_p^{(2)}(z^3)$	$\rho_p^{(2)}(z^4)$	$\rho_p^{(2)}(z^5)$	$\rho_p^{(2)}(z^6)$
1.16355181	1.07917607	1.08928688	1.05724264	1.23662075	1.20500141
$\rho_p^{(2)}(z^7)$	$\rho_p^{(2)}(z^8)$	$\rho_p^{(2)}(z^9)$	$\rho_p^{(2)}(z^{10})$	$\rho_p^{(2)}(z^{11})$	$\rho_p^{(2)}(z^{12})$
1.05068226	1.23700720	1.08465280	1.05214443	1.20777991	1.07391514
	$\mu_p^{(3)}(z)$	$\mu_p^{(4)}(z)$	$\mu_p^{(5)}(z)$	$\mu_p^{(6)}(z)$	
	1.18703055	1.17341339	1.20657887	1.17384728	

There is no other primitive root z that fulfills the condition $\rho_p^{(2)}(z^k) < 1.25$ for $1 \le k \le 12$ with $\mu_p^{(l)}(z) < 1.25$ for $3 \le l \le 6$.

The second best will be $z' = 1877882398 \equiv 7^{1007706005} \ (\mathrm{mod} p)$, with $(z')^{-1} \equiv 1589301084 \equiv 7^{1139777641} \ (\mathrm{mod} p)$ with the following performance.

$\rho_p^{(2)}(z')$	$\rho_p^{(2)}(z'^2)$	$\rho_p^{(2)}(z'^3)$	$\rho_p^{(2)}(z'^4)$	$\rho_p^{(2)}(z'^5)$	$\rho_p^{(2)}(z'^6)$
1.11485212	1.06100477	1.13071832	1.16364991	1.08706105	1.15812695
$\rho_p^{(2)}(z'^7)$	$\rho_p^{(2)}(z'^8)$	$\rho_p^{(2)}(z'^9)$	$\rho_p^{(2)}(z'^{10})$	$\rho_p^{(2)}(z'^{11})$	$\rho_p^{(2)}(z'^{12})$
1.08675921	1.20197885	1.05820553	1.13034603	1.75265194	1.08722175
	$\mu_p^{(3)}(z')$	$\mu_p^{(4)}(z')$	$\mu_p^{(5)}(z')$	$\mu_p^{(6)}(z')$	
	1.10857780	1.23478898	1.04578463	1.23920574	

use, including optimizations, or even corrections if any, watching the **Notices** at the end of this report.

[9]The consecutive l-tuples of integers from a (d, z) generator form the so-called (d, z) lattice. The largest distance between parallel and neighboring lattice htperplanes is denoted $\lambda_d^{(l)}(z)$. The performance of a (d, z) generator is assessed by the ratio $\rho_d^{(l)}(z) := \lambda_d^{(l)}(z)/\overline{\lambda}_d^{(l)}$ or by $\mu_d^{(l)}(z) := \lambda_d^{(l)}(z)/\overline{\mu}_d^{(l)}$ with reference values $\{\overline{\lambda}_d^{(l)}, \overline{\mu}_d^{(l)}\}$ to be given later in footnote14. The performance of a generator is better if noted valuations are closer to 1 from above. For more details on the meaning of these valuations, readers are referred to Nakazawa and Nakazawa (2008) in the footnote 5. This reference will also give the intuitive, geometrical understanding of the 2nd degree valuations $\rho_d^{(2)}(z) = \mu_d^{(2)}(z)$. For $\mu_d^{(l)}(z)$ of newly introduced spectral tests with degree $l \ge 3$, see Nakazawa and Nakazawa (2014a) cited in footnote 4. Also, Nakazawa and Nakazawa (2015) in footnote 4, *The geometry of spectral tests*, will give clear overviews on the problem.

[10]The multiplier 7 is the smallest primitive root of p; the program to compute these data is as follows.

```
implicit integer*8(a-z)
d=2147483647
base=7
z=318320879
y=1
    j=0
10  x=y*base
    y=mod(x,d)
    j=j+1
    if (y.eq.z) goto 20
    goto 10
20  print*,' z =',y,' log(z) =',j,' base =',base
    stop
    end
```

These star multipliers are recommended for computing, if their period $T = \varphi(p)/2 = 1073741823$ is practicable.[11] Sorry to say, our desktop computers of today use up these whole period T within 30 seconds and, moreover, random numbers generated in this way can have only the single precision as real numbers. Large scale simulations of today will require $T \approx 2^{52}$, together with the double precision.[12] Devices of two-odd-prime moduluses will now be indispensable in design.

It should be warned that almost all of primitive roots give bad *random numbers*. And we have to show a seemingly very good multiplier, which nevertheless cautions us about possible disasters. Under the same prime modulus $d = p = 2147483647$ the primitive root multiplier $z'' = 1882878852 \equiv 7^{737502841} \pmod{p}$ has the following performance.

$\rho_p^{(2)}(z'')$	$\rho_p^{(2)}(z''^2)$	$\rho_p^{(2)}(z''^3)$	$\rho_p^{(2)}(z''^4)$	$\rho_p^{(2)}(z''^5)$	$\rho_p^{(2)}(z''^6)$
1.04297913	1.09683384	1.15760026	1.09170464	1.04741575	5.20055942
$\rho_p^{(2)}(z''^7)$	$\rho_p^{(2)}(z''^8)$	$\rho_p^{(2)}(z''^9)$	$\rho_p^{(2)}(z''^{10})$	$\rho_p^{(2)}(z''^{11})$	$\rho_p^{(2)}(z''^{12})$
1.21701307	1.07163895	1.04891059	1.09439741	1.47956601	2.31913189
	$\mu_p^{(3)}(z'')$	$\mu_p^{(4)}(z'')$	$\mu_p^{(5)}(z'')$	$\mu_p^{(6)}(z'')$	
	1.20945690	1.15753720	1.24082594	1.16444381	

What is happening here on the sequence $\{(v_j, v_{j+1}, v_{j+2}, \cdots, v_{j+6}) |\ j = 1, 2, \cdots\}$ of $k + 1 = 7$ consecutive random numbers? We still cannot say anything certain. But one thing is for sure. We would like to use the best performer $z = 318320879$, and we should avoid the danger of using this one.

Concludingly, we may raise several general morals obtained.

(A) The extended 2nd degree spectral tests are versatile in sieving out generators with faults. At least, the 2nd degree spectral tests of (d, z^k) for $1 \le k \le 6$ will be necessary.

(B) The revised 3rd to 6th spectral tests based on valuations $\{\mu_d^{(k)}(z) |\ 3 \le k \le 6\}$ will doubtlessly be the appropriate technique, to replace the prior arts based on the conclusions of the Geometry of Numbers. And, to our pleasure, the present example with the Mersenne prime $p = 2^{31} - 1$ modulus shows that revised spectral tests enable us to find generators of excellence far more abundantly. This will be experienced with other types of moduluses and their primitive root multipliers.

(C) However, (d, z) generators formed by single prime moduluses cannot successfully be extended to multiplicative congruential generators with sufficiently long period T at

[11] The period L of the multiplicative random number sequence generated by any primitive root z is the largest possible $\varphi(p) = p - 1$. However, at $T = L/2$ there arises $z^T \equiv -1 \pmod{p}$, and the rest of the sequence is essentially the repetition of the first half. Therefore, only the half length $T = L/2 = \varphi(p)/2$ is usable for *independent* random numbers.

[12] The period $T \approx 2^{52}$ will be used up in our small computers in about 2 years.

present. The matter does not improve with moduluses of the type $d = 2^i$, which has the flaw of periodic behavior of generated random numbers in their insignificant bits. This is the reason that they cannot be combined with moduluses of odd primes or odd-prime-powers, as found in Nakazawa and Nakazawa (2008).[5] The use of two odd-prime-factor moduluses d_1 and d_2 is indispensable, and we should combine two such subgenerators (d_1, z_1) and (d_2, z_2) by Sun Tzu's theorem. This whole forms a system of very laborious and time-consuming tasks, though the success is not impossible. The process has little chance with only a few excellent subgenerators $\{(d_k, z_k)|\ k = 1, 2, \cdots\}$. We in fact needed[13] tens of thousands of excellent sub-generators in order to find a dozen of successful combinations. The search should include many primes or their powers for moduluses, and exhaust all possible multipliers of respective primes or their powers. The Mersenne prime $p = 2^{31} - 1$ seems to give too many prime factors for its period $\varphi(p) = p - 1$, which are well-known to be $\{2, 3, 7, 11, 31, 151, 331\}$. We recommend a more restricted class of primes that give easier search of their primitive roots together with other favorable structures. See *invention1a.pdf* cited as Nakazawa and Nakazawa (2014) in footnote 3.

Notices. The method of extended 2nd degree spectral tests of (d, z^k) for $k \geq 2$ and the method of revised l-th degree spectral tests based on the new reference values[14] were filed for Patent applications.

As announced, the fortran 90 file *fishmanmoorenao.for* for the present computation and its output file *fishmanmoorenao.txt* are posted in this URL in downloadable forms. Interested readers are advised to run the program on their computers to see the scenery played by integers. Readers may make free personal use of this program, including their respective devices for optimizaion and corrections, if any, of course. But please watch the above noted announcements of filing for Patent applications.

---

[13] See *The Prospectus of Nakazawa Patents* noted in footnote 6 for such successful combinations.

[14] These *regular simplex* reference values, to be denoted as $\{\overline{\mu}_d^{(l)}\}$ including the case $l = 2$, may be compared as follows to $\{\overline{\lambda}_d^{(l)}|\ l \geq 2\}$, which were given by the Geometry of Numbers and used by Fishman and Moore:

$$0.93060d^{1/2} \approx \overline{\mu}_d^{(2)} := 2^{-1/2}3^{1/4}d^{1/2} = \overline{\lambda}_d^{(2)},$$
$$0.91649d^{2/3} \approx \overline{\mu}_d^{(3)} := 3^{-1/2}4^{2/6}d^{2/3} > \overline{\lambda}_d^{(3)} := 2^{-1/6}d^{2/3} \approx 0.80909d^{2/3},$$
$$0.91429d^{3/4} \approx \overline{\mu}_d^{(4)} := 4^{-1/2}5^{3/8}d^{3/4} > \overline{\lambda}_d^{(4)} := 2^{-1/4}d^{3/4} \approx 0.84090d^{3/4},$$
$$0.91575d^{4/5} \approx \overline{\mu}_d^{(5)} := 5^{-1/2}6^{4/10}d^{4/5} > \overline{\lambda}_d^{(5)} := 2^{-3/10}d^{4/5} \approx 0.81225d^{4/5},$$
$$0.91844d^{5/6} \approx \overline{\mu}_d^{(6)} := 6^{-1/2}7^{5/12}d^{5/6} > \overline{\lambda}_d^{(6)} := 2^{-1/2}3^{1/12}d^{5/6} \approx 0.77490d^{5/6}.$$

Addenda (September 29, 2015)

To our dismay, bugs were found in the program *fishmanmoorenao.for* posted in this URL. The file was corrected to *fishmanmoorenaonew.for*, so as to be applied safely by any users, and uploaded in this URL together with its new output file *fishmanmoorenaonew.txt*. Old and new output files were examined by a program *fmnreader.for* also uploaded here, and gave a happy conclusion that only one primitive root in the old *fishmanmoorenao.txt* needs a correction in its 6th data. There is no other flaw in both files. This luck might well seem miraculous, but there are reasons. Let us elucidate the matter step by step.

In the way advocated by present authors, the l-th degree spectral test of a (d, z) generator works to find the shortest *dual* lattice vector $\boldsymbol{f} = (y_1, y_2, \cdots, y_l)$ with integer coordinates by sweeping over all vectors in the range given by reference values[14] $\{\overline{\lambda}_d^{(l)}, \overline{\mu}_d^{(l)} \mid l = 2, 3, \cdots\}$,

$$d/\overline{\lambda}_d^{(l)} > \|\boldsymbol{f}\| > d/(1.25\overline{\mu}_d^{(l)}), \quad l \geq 2, \quad \overline{\lambda}_d^{(2)} = \overline{\mu}_d^{(2)}, \quad \|\boldsymbol{f}\| = ({y_1}^2 + {y_2}^2 + \cdots + {y_l}^2).$$

The program *fishmanmoorenao.for* adopted a narrower range

$$\left(d/\overline{\lambda}_d^{(l)} >\right) d/\overline{\mu}_d^{(l)} > \|\boldsymbol{f}\| \left(> d/(1.25\overline{\lambda}_d^{(l)})\right) > d/(1.25\overline{\mu}_d^{(l)}), \quad l \geq 3,$$

expedite the search process. This was incorrect. Nevertheless, why could it be so successful as to give almost all correct results excepting only one z? A comprehension is obtained by

$p = 2147483647 \quad z = 334030676$ (inaccuracy in $\mu_p^{(6)}(z)$)

$\rho_p^{(2)}(z)$	$\rho_p^{(2)}(z^2)$	$\rho_p^{(2)}(z^3)$	$\rho_p^{(2)}(z^4)$	$\rho_p^{(2)}(z^5)$	$\rho_p^{(2)}(z^6)$
1.10910130	1.13880330	1.22974675	1.09192351	1.01935750	2.88012129
$\rho_p^{(2)}(z^7)$	$\rho_p^{(2)}(z^8)$	$\rho_p^{(2)}(z^9)$	$\rho_p^{(2)}(z^{10})$	$\rho_p^{(2)}(z^{11})$	$\rho_p^{(2)}(z^{12})$
1.38091312	1.69127299	1.09570529	1.43761825	4.57276121	7.48676688
	$\mu_p^{(3)}(z)$	$\mu_p^{(4)}(z)$	$\mu_p^{(5)}(z)$	$\mu_p^{(6)}(z)$	
	1.19307912	1.19844004	1.08566596	1.00000000	

$p = 2147483647 \quad z = 334030676$ (correct)

$\rho_p^{(2)}(z)$	$\rho_p^{(2)}(z^2)$	$\rho_p^{(2)}(z^3)$	$\rho_p^{(2)}(z^4)$	$\rho_p^{(2)}(z^5)$	$\rho_p^{(2)}(z^6)$
1.10910130	1.13880330	1.22974675	1.09192351	1.01935750	2.88012129
$\rho_p^{(2)}(z^7)$	$\rho_p^{(2)}(z^8)$	$\rho_p^{(2)}(z^9)$	$\rho_p^{(2)}(z^{10})$	$\rho_p^{(2)}(z^{11})$	$\rho_p^{(2)}(z^{12})$
1.38091312	1.69127299	1.09570529	1.43761825	4.57276121	7.48676688
	$\mu_p^{(3)}(z)$	$\mu_p^{(4)}(z)$	$\mu_p^{(5)}(z)$	$\mu_p^{(6)}(z)$	
	1.19307912	1.19844004	1.08566596	0.99820306	

closer observations of the pertinent multiplier $z = 334030676$. Two lists shown above were obtained by applying the program *fmnreaderev.for* which shows the difference of two files, and also spectral test valuations that are less than or equal to 1. The results show that the above lists are the *sole* difference between two output files; the lower, correct list shows also that the 6th degree tests have conspicuously the valuation smaller than 1.[15] Thinking on bugs in *fishmanmoorenao.for*, we are surprised by this small inaccuracy. The true implication of this result will be the powerul role of extended 2nd degree tests over (d, z^k) for $2 \le k \le 5$ adopted in these programs assisting the 2nd degree test of (d, z). Note typically that if we tighten the requirement for (d, z^k) to pass the 2nd test for $1 \le k \le 6$, then this multiplier z is retired from the list automatically in both programs, leaving at the same time only passers with all valuations greater than 1.

It will be in order to consider the historical 5 excellent multipliers, found by Fishman and Moore (1986) for the present prime modulus $d = 2^{31} - 1$, under the extended 2nd degree tests for (d, z^k) and 3rd to 6th degree tests based on $\{\overline{\mu}_d^{(l)} | \ 3 \le l \le 6\}$. The fortran90 program *fishmanmoorenaonew.for* may readily be used to this end by putting its variable kflag to be 1, which frees (d, z) from the 1.25 restrictions. Lists below give their performances.

$$p = 2147483647 \quad z = 742938285$$

$\rho_p^{(2)}(z)$	$\rho_p^{(2)}(z^2)$	$\rho_p^{(2)}(z^3)$	$\rho_p^{(2)}(z^4)$	$\rho_p^{(2)}(z^5)$	$\rho_p^{(2)}(z^6)$
1.15306751	1.91805599	1.81316446	1.32378868	3.25782855	1.04479227
$\rho_p^{(2)}(z^7)$	$\rho_p^{(2)}(z^8)$	$\rho_p^{(2)}(z^9)$	$\rho_p^{(2)}(z^{10})$	$\rho_p^{(2)}(z^{11})$	$\rho_p^{(2)}(z^{12})$
1.27061834	1.51793133	1.08552006	1.05089118	3.88226372	1.63799806
	$\mu_p^{(3)}(z)$	$\mu_p^{(4)}(z)$	$\mu_p^{(5)}(z)$	$\mu_p^{(6)}(z)$	
	1.12942799	1.06610522	1.06615156	1.01146880	

$$p = 2147483647 \quad z = 950706376$$

$\rho_p^{(2)}(z)$	$\rho_p^{(2)}(z^2)$	$\rho_p^{(2)}(z^3)$	$\rho_p^{(2)}(z^4)$	$\rho_p^{(2)}(z^5)$	$\rho_p^{(2)}(z^6)$
1.16627569	1.19708825	6.76681886	1.46420589	5.00940631	2.26206864
$\rho_p^{(2)}(z^7)$	$\rho_p^{(2)}(z^8)$	$\rho_p^{(2)}(z^9)$	$\rho_p^{(2)}(z^{10})$	$\rho_p^{(2)}(z^{11})$	$\rho_p^{(2)}(z^{12})$
1.21334088	1.06699900	1.48651874	1.20783026	1.62042788	2.94366623
	$\mu_p^{(3)}(z)$	$\mu_p^{(4)}(z)$	$\mu_p^{(5)}(z)$	$\mu_p^{(6)}(z)$	
	1.08184373	1.05818358	1.06390229	1.01968669	

[15] At the same time we confirm that no other multiplier z has its valuations smaller than or equal to 1 in both outputs.

$p = 2147483647 \quad z = 1226874159$

$\rho_p^{(2)}(z)$	$\rho_p^{(2)}(z^2)$	$\rho_p^{(2)}(z^3)$	$\rho_p^{(2)}(z^4)$	$\rho_p^{(2)}(z^5)$	$\rho_p^{(2)}(z^6)$
1.18893209	3.51885751	2.19846315	1.15368543	1.47158421	1.48916585
$\rho_p^{(2)}(z^7)$	$\rho_p^{(2)}(z^8)$	$\rho_p^{(2)}(z^9)$	$\rho_p^{(2)}(z^{10})$	$\rho_p^{(2)}(z^{11})$	$\rho_p^{(2)}(z^{12})$
2.71954704	1.48917422	1.26686164	1.04170825	1.14088492	1.51863760
	$\mu_p^{(3)}(z)$	$\mu_p^{(4)}(z)$	$\mu_p^{(5)}(z)$	$\mu_p^{(6)}(z)$	
	1.10626650	1.11416388	1.05870887	0.99917993	

$p = 2147483647 \quad z = 62089911$

$\rho_p^{(2)}(z)$	$\rho_p^{(2)}(z^2)$	$\rho_p^{(2)}(z^3)$	$\rho_p^{(2)}(z^4)$	$\rho_p^{(2)}(z^5)$	$\rho_p^{(2)}(z^6)$
1.11986188	1.79072973	1.44118579	1.20332225	1.17058675	1.63022644
$\rho_p^{(2)}(z^7)$	$\rho_p^{(2)}(z^8)$	$\rho_p^{(2)}(z^9)$	$\rho_p^{(2)}(z^{10})$	$\rho_p^{(2)}(z^{11})$	$\rho_p^{(2)}(z^{12})$
1.11012704	1.74530778	1.15721717	1.06989042	3.91997548	1.80176928
	$\mu_p^{(3)}(z)$	$\mu_p^{(4)}(z)$	$\mu_p^{(5)}(z)$	$\mu_p^{(6)}(z)$	
	1.09184334	1.07254554	1.02780319	1.02282044	

$p = 2147483647 \quad z = 1343714438$

$\rho_p^{(2)}(z)$	$\rho_p^{(2)}(z^2)$	$\rho_p^{(2)}(z^3)$	$\rho_p^{(2)}(z^4)$	$\rho_p^{(2)}(z^5)$	$\rho_p^{(2)}(z^6)$
1.21411121	1.99192650	1.45479150	1.13241226	1.56904222	1.04455900
$\rho_p^{(2)}(z^7)$	$\rho_p^{(2)}(z^8)$	$\rho_p^{(2)}(z^9)$	$\rho_p^{(2)}(z^{10})$	$\rho_p^{(2)}(z^{11})$	$\rho_p^{(2)}(z^{12})$
1.88757973	2.47412478	1.33757462	2.01696843	1.06350404	2.05652288
	$\mu_p^{(3)}(z)$	$\mu_p^{(4)}(z)$	$\mu_p^{(5)}(z)$	$\mu_p^{(6)}(z)$	
	1.16776058	1.11553861	1.07356141	1.02212156	

We see that the multiplier $z = 1226874159$ has the valuation $\mu_p^{(6)}(z) = 0.99917993 < 1$. Second degree valuations demand us to conclude this as well as other multipliers are inadequate in the new criterion for uniform and independent random numbers.

Stepping back to the general ocerview, we note that the consecutive l-tuples from the (d, z) multiplicative congruential generators form points in the l-dimensional Euclidean space E_l,

$$\{P_j :\equiv (z^j, z^{j+1}, z^{j+2}, \cdots, z^{j+l-1}) \,(\mathrm{mod} d) |\; j = 0, 1, 2, \cdots\}.$$

These are known to be on lattice points of a lattice, called the (d, z) lattice. Its any set of basis vectors form the l-simplex,[16] which constitutes so-called unit cells of the lattice.

[16] In the plane E_2 with $l = 2$ the 2-simplex is the triangle spanned by 2 basis vectors. In E_3 the 3-simplex is the tetrahedron spanned by 3 basis vectors.

Nakazawa and Nakazawa (2014a)[3] discussed that a lattice with basis vectors forming a *regular* l-simplex provides the most favorable geometry of seats for (d, z) lattice in E_l, in order for (d, z) generator to *appear* to give *independent* random numbers. This recognition was the motive to advocate regular simplex reference values $\{\overline{\mu}_d^{(l)} \mid l = 2, 3, \cdots\}$ for spectral tests. Any lattice in E_l has parallel and neighboring $(l-1)$-dimensional lattice hyperplanes. The largest value $\lambda_d^{(l)}(z)$ of distances between parallel and neighboring lattice hyperplanes gives the ratio $\mu_d^{(l)}(z) := \lambda_d^{(l)}(z)/\overline{\mu}_d^{(l)}$ for $l \geq 3$ or $\rho_d^{(2)}(z) := \lambda_d^{(2)}(z)/\overline{\lambda}_d^{(2)}$. These are lth degree and 2nd degree spectral test valuations of the (d, z) generator. Thus, $\mu_d^{(l)}(z)$ close to 1 will suggest that the (d, z) lattice in E_l is close in form to the regular lattice constituted by basis vectors forming regular l-simplexes. This idea is natural. However, we need here to think deeper on geometrical circumstances.

Let there be a regular l-simplex; the image of a regular tetrahedron or more simply the regular triangle will be useful. Consider a small deformation of this l simplex to a non-regular form keeping the (hyper)volume at a constant value. Let any hypersurface of this l-simplex have the hyperarea S, and the vertex of the l-simplex facing S have the height h from S. The volume of the l-simplex is $hS/l!$ as known. In the noted deformation all of its hypersurfaces cannot increase unanimously (nor cannot decrease unanimously). Necessarily there should arise some hypersurface S that diminishes its hyperarea and the vertex facing it should increase its height h. The largest height of the deformed l-simplex is the largest distance between parallel and neighboring lattice hyperplanes. Therefore, in all small deformations of a (d, z) lattice in the vicinity of the regular l-simplex lattice, the valuation $\mu_d^{(l)}(z)$ should be larger than 1.[17] In this sense, the valuation $\mu_d^{(l)}(z) \leq 1$ implies that the (d, z) lattice is rather remote from the form of a regular lattice, and not adequate as seats of points formed by consecutive l-tuples of *independent* random numbers.

We proposed in spectral tests of (d, z) generators to discard such (d, z) generators with the valuation $\mu_d^{(l)}(z)$ smaller than 1, however close the value may be from below. We would discard such (d, z) generators with $\mu_d^{(l)}(z) \leq 1$. All examples we have seen support this choice as technological wisdom.

It is gratifying that 2nd degree spectral tests of (d, z^k) for $2 \leq k \leq 6$, besides the classical $k = 1$ case, work very efficiently in sieving out (d, z) generators with undesirable lattice geometries. They deserve higher respects than ever. After all, they are the lightest and the fastest members in spectral test families.

[17] The equation $\mu_d^{(l)}(z) = 1$ cannot arise in the (d, z) lattice formed by basis vectors with integer coordinates.