Lounge A: Disclosure: 2024/2/8

Two Excellent MC Generators

Naoya Nakazawa/ Hiroshi Nakazawa

Hirakata Ransu Factory (HRF)

1. On Criterions of Random Number Generators

The multiplicative congruential (MC) random number generators are defined by 3 integers (d, z, n), $d > 0$ for the modulus, z coprime with d for the multiplier and n for the seed also coprime with d. Without loss of generality we may take $1 \leq n < d$ for the seed, which determines the start of the sequence of random numbers, and has no relation to the *excellence* of the emitted random numbers. We take hereafter that (d, z) are key quantities for MC random number gerators. All these matters are detailed in our completed monograph *Random Number Generators on Computers*, which is to be published soon. So we abbreviate arguments on structures of MC generators as well as on criterions for the excellence of generators, go straightly into dexcriptions of 2 excellent MC generators, and wish to enable readers to test these generators by themselves.

2. Generator #001, the Present Best

The HRF was lucky to find the generator named #001 first of all in November of 2018, by the computing of Naoya Nakazawa. After 6 years it is on the top of generators found. The generator employs the modulus formed by 2 Sophie German (SG) primes giving a large period $T \approx 2^{52}$. As a sincere service to any scientist and creator in any nation, we HRF disclose its constitution.

Table A. The structure of #001

$d = p_1 p_2 = 18055400005099021 \approx 2^{54.00}$

SG prime $p_1 = 134265023 \approx 2^{27.00}$

SG prime $p_2 = 134475827 \approx 2^{27.00}$

the primitive root z_1 of p_1: $\quad z_1 = 19061252 \approx 2^{24.18}$

the primitive root z_2 of p_2: $\quad z_2 = 77600525 \approx 2^{26.21}$

composite multiplier by Sunzi theorem:

$$z \equiv 7759097958782935 \approx 2^{52.79}$$

usable LCM period T:

$$T = \mathrm{LCM}(p_1 - 1, p_2 - 1)/2 = 4513849934089543 \approx 2^{52.00}$$

multipliers with the same T and test valuations:

$$\begin{aligned} z^{-1} &\equiv 8723774547862110 \approx 2^{52.95} \\ -z &\equiv 10296302046316086 \approx 2^{53.19} \\ -z^{-1} &\equiv 9331625457236911 \approx 2^{53.05} \end{aligned}$$

(End of Table A)

List B shown below gives test valuations of #001 in generalized 2nd tests which are to be larger than 1.00. If valuations are within 1.25, the generator is passable as pair of outputs with $2, 3, \cdots, 8+1$ steps apart have no sizable pair correlations.

List B. Generalized 2nd test valuations of #001
in its 2nd tests for $(d, z^1), (d, z^2), \cdots, (d, z^{11})$

1.08678338 1.23476055 1.09373237 1.14778981 1.13682785
1.16390618 1.09784908 1.21656428 1.52552804 1.34934813
7.69460527

(End of List B)

Explanations of these minute details are not easy in these brief comments. Readers are referred to our monograph, *Random Number Generators on Computers*, now finished of proofs and to be published, for the full detailes.

As the next come *regular simplex criterion spectral test valuations.*

The ideal lattice geometry, formed by consecutive outputs of random number generators with uniform and independent statistics, was corrected to regular lattice with regular simplex unit cells. For dimensions larger than 2, these unit cells cannot have the smallest possible edge lengths.[1] In below we show these revised spectral test valuations of #001.

List C. Regular simplex valuations of #001 for 3rd to 6th degrees

$$1.13600074 \quad 1.04031015 \quad 1.10996227 \quad 1.21389160$$

(End of List C)

Below in **List D** we present results of edge tests. They show ranges of edge lenghs of *the most compact simplex* in the lattice formed by consecutive k random numbrs. Namely, we take the shortest k distances of lattice points which form a linearly independent lattice vectors. Linear independence is proven by their non-zero determinant which may be computed by real arithmetic.[2] Computing all edge lengths of the simplex formed by these k shortest lattice vectors, we have the shortest and *presumably* the longest edge lengths. The degrees of deformation of the lattice is informed by dividing the one and the same length l of the regular lattice shortest vectors, The values shown below gives l divided by the longest vector length of #001 (on the left) and l divided by the shortest vector length[3] of #001 (on the right).

[1] H. Nakazawa and N. Nakazawa: *Method of Spectral Tests of Multiplicative Congruential Random Number Generators,* on *www10.plala,or,jp/h-nakazawa/indexarchive (2014).* In this revised criterion, we obtained for the first time a generator formed by 2 *excellent* subgenerators (p_1, z_1) and (p_2, z_2) can give a generator with the composite modulus $d = p_1 p_2 \approx 2^{54}$ giving *excellent statistics.*

[2] In fact, the determinant is computed easily without pivoting in double precision real arithmetic. The determinant is large d^{l-1} for the l-dimensional lattice formed by consecutive l MC random numbers. We used the $l+1$ shortest lattice vectors to select linearly independent set. So, the computed longest edge length is the upper limit, and the true longest lattice vectors can be not as long as the tests give; but this is no harm to the longest edge test.

[3] This length is precisely true.

List D. Longest and shortest edge test valuations of #001

(3rd degree)	0.78489424	1.18938572
(4th degree)	0.73780699	1.17913686
(5th degree)	0.83524952	1.20173353
(6th degree)	0.71002135	1.20574247

(End of List D)

The most remarkable point is that the probram to generato MC random numbers proceeds only in integer*8 and real*8 arithmetic.[4] The CPU time for this 10 million outputs is about 0.281s on our middle speed computer. Random number outputs have the sufficient real*8 precision $1/d \approx 2^{-54}$. The usable period of the generator is about 2^{52}. The generation of the whole period $T \approx 2^{52}$ will take 2 years on our desktop computers. Computing programs of #001 is shown in the next page as **Figure E**.

Tne details of structures arising with tests of #001 are intricate, and short comments presented here might well be in sufficient. Our monograph *Random Number Generators on Computers* was under repeated pfoof, and is now believed to be complete. It is to be published, hopefully soon. Please refer to this monograph for other details of subjects.

[4] This implication of Sunzi theorem was discovered by Naoya Nakazawa. Readers are referred to Naoya Nakazawa and Hiroshi Nakazawa: English translation of a Patent Application to Japan Patent Office, June 13 of 2022, *Sunzi Reduction to Compute Multiplicative Congruential Random Numbers with Composite Moduluses*, in *http://www10.plala.or.jp/h-nkzw/indexarchive22june13.html.*

List E. Computing Programs for #001

```
program main
implicit integer*8(i-n), real*8(a-h,o-z)
common ip1,ip2,id,ad,iz1,iz2,mz1,mz2,ip2mp1,ip1mp2
ip1=134265023
ip2=134475827
id=ip1*ip2   ! id $\approx 2^{54}$
ad=id
iz1=19061252
iz2=77600525
n1=10
n2=13
ip2mp1=52577007
ip1mp2=81816271
iseed1=n1 ! integer*4 to assign iseed1=mod(iseed,ip1)
iseed2=n2 ! integer*4 to assign iseed2=mod(iseed,ip2)
mz1=iseed1
mz2=iseed2
do i=1,10000000
call random(rand)
end do
        . . . . . . . . . . . . . . . . . .
end    !(main program end)

subroutine random(rand)
implicit integer*8(i-n), real*8(a-h,o-z)
common ip1,ip2,id,ad,iz1,iz2,mz1,mz2,ip2mp1,ip1mp2
mz1=mod(mz1*iz1,ip1)
mz2=mod(mz2*iz2,ip2)
mz1a=mod(mz1*ip2mp1,ip1)
mz2a=mod(mz2*ip1mp2,ip2)
az=mod(ip2*mz1a+ip1*mz2a,id)
rand=az/ad
return
end
```

(End of List E)

For the confirmation we list below 100 outputs emitted from #001 after outputting 10^7 random numbers according to **Figure E**.

List F. 100 Outputs from #001 generator

```
0.653816355434 0.162395903492 0.666319058508 0.192823573723
0.489788498203 0.327381692216 0.006207372410 0.817190447249
0.639382522876 0.999243182851 0.717807517328 0.582888069563
0.751959446280 0.456610909409 0.201265518413 0.197352588136
0.185468833692 0.026325012527 0.798951425190 0.980168183205
0.728774197785 0.895636674003 0.746279846438 0.334966215203
0.163132201425 0.161807776678 0.478463418819 0.402555313497
0.412925462471 0.228549325709 0.116935094385 0.887686052660
0.748053624507 0.372387517800 0.401887611920 0.513438563398
0.218008135464 0.479107340785 0.371799991246 0.610473874869
0.495998588197 0.704020149239 0.125946074052 0.689497113384
0.296979898817 0.664141855353 0.967378082658 0.861373665256
0.146986132091 0.320681156594 0.293103638455 0.410906693576
0.830103955630 0.320270139018 0.924042828676 0.087350373543
0.943936287549 0.994736329597 0.408045545191 0.472523592537
0.765124568761 0.630798202897 0.873021775270 0.612753906188
0.124335863299 0.816173368849 0.470611672694 0.880574814564
0.668048788679 0.380757635873 0.439593072176 0.532108985606
0.235689661806 0.023857729188 0.606829757993 0.762549693572
0.627268755976 0.592982603016 0.803692768860 0.555192595035
0.568754093418 0.482014270564 0.450138517310 0.960974827043
0.500236510179 0.285096197971 0.920893782638 0.842851188064
0.083495098650 0.555523403307 0.712500499476 0.525529497885
0.921528283135 0.667901000917 0.272780491599 0.962922804725
0.924506422608 0.495041819614 0.783468131560 0.851983710989
```

(End of List F)

3. A Large Scale Excellent MC Generator #003

The generator #003 was found by Naoya Nakazawa in April of 2020. Please guess how rarely good MC generators are found.[5] Its modulus $d = p_1 p_2$ is formed by 2 NN primes p_1, p_2. Test valuations are almost comparable to #001, but please note the slightly inferior generalized 2nd tests. The usable LCM period of #003 is $T \approx 2^{51}$ which is a little smaller than #001, as subgenerators (p_1, z_1) and (p_2, z_2) both have a common factor 2 in their usable periods. Putting aside these small drawbacks, #003 will be a good alternative of #001, with following structures.

List G. Generator #003 on 2 NN prime moduous

Modulus $d = p_1 p_2 = 18015370515269401 \approx 2^{54.000}$
NN subprime $p_1 = 134224829 \approx 2^{27.000}$
NN subprime $p_2 = 134217869 \approx 2^{27.000}$
primitive root submultiplier $z_1 = 95967890 \approx 2^{26.516}$ of p_1 and
primitive root submultiplier $z_2 = 4256141 \approx 2^{22.021}$ of p_2
Sunzi multiplier $z = 16048994718289548 \approx 2^{53.833}$
usable period $T = 2251921280853338 \approx 2^{51.000}$
multipliers sharing usable period and test valuations

$$\begin{aligned} z^{-1} &\equiv 10990185200333827 \approx 2^{53.29} \\ -z &\equiv 1966375796979853 \approx 2^{50.80} \\ -z^{-1} &\equiv 7025185314935574 \approx 2^{52.64} \end{aligned}$$

(End of List G)

Generalized 2nd degree spectral tests run as follows.

List H; Generalized 2nd tests for (d, z^2)-(d, z^{11})

1.12378644 1.22759925 1.15381455 1.07582363 1.12113014
1.90830600 2.56595210 1.64729694 1.10578807 1.10728840
2.12669792

(End of List H)

The next **List I** gives valuations of #003 in regular simplex spectral

[5] We should let 10 or more cores of computers run 24 hours without rest, wasting sizable electric powers without any success.

tests of 3rd to 6th degrees.

List I. Regular Simplex 3rd-6th Spectral Tests of #003

1.14537815 1.06716995 1.13487872 1.21563615

The final list is the test valuations of #003 in the longest edge tests (on the left) and the shortest edge tests (on the right) for 3rd to 6th degrees.

List J. Longest and Shortest Edge Tests of 3rd to 6th Degrees

(3rd Degree)	0.77772641	1.16750024
(4th Degree)	0.74018574	1.20907497
(5th Degree)	0.68729723	1.23300972
(6th Degree)	0.69782364	1.23425488

In sum, valuations are excellent with #003. The generalized 2nd degree tests pass up to the 5th degree, which is a little behind the 8th of #001. We again stress that #003 is a good alternative of #001.

Please refer to **List E** of computing program for #001. A simple set of replacements

ip1 =	134224829	ip2 =	134217869
iz1 =	95967890	iz2 =	4256141
ip2mp1 =	72300127	ip1mp2 =	61921491

will change all for #003.