Sunzi Reduction Caldulus for Multiplicative Congruential Random Numbers

Naoya Nakazawa[1] / **Hiroshi Nakazawa**[1]

(May 27, 2024)

An invention is disclosed on a class of multiplicative congruential (MC) random number generators with moduluses formed by two mutually coprime submoduluses. The generator gives MC sequences with usable periods of 2^{54} or larger. Yet they admit very fast computing, by a way of decomposition given by Sunzi theorem. The present invention is concerned with cases of very large moduluses, and magical Sunzi theorem shows its own novel facet. In the presented method the MC random number generators use only the arithmetic of double precision integers (not exceeding 2^{64}) and double precision reals, yet respecting the reproducibility and the transportability of generated random numbers.

[0001] We present here a new class of fast MC random number generator (d, z, n), with the integer $d > 0$ called *modulus*, with the integer z called *multiplier* coprime to d in the range $0 < z < d$, and with the integer n called *seed* also coprime to d and in the range $0 < n < d$. The MC generator (d, z, n) gives the sequence of random integers $\{X_0, X_1, X_2, \cdots\}$ in the open interval $(0, d)$, in the recursive fashion

$$X_0 = \mathrm{mod}(n,\, d), \quad X_{k+1} = \mathrm{mod}(zX_k,\, d), \quad k = 0, 1, 2, \cdots.$$

Noted procedure of generation may also be given as

$$\{X_k = \mathrm{mod}(nz^k,\, d) |\ \ k = 0, 1, 2, \cdots\}.$$

Hereafter the function $\mathrm{mod}(A,\, d) = R$ is defined on any non-negative integer A as the integer remainder R in $[0, d)$ obtained when A is divided by d. The definition may be made quantitative in the equation of division of A by d with a non-negative integer quotient Q,

$$A = Qd + R, \quad \text{non-negative integer } R < d \text{ is the remainder.}$$

As the function $\mathrm{mod}(A,\, d)$ should inevitably be used in computing, we need to be accustomed to its use. However, the above definition as the mathematical logic is not neat. Please think over the abstruse Sunzi theorem, and allow for our desperate efforts.

[0002] The MC uniform *(rational)* random numbers distributed in the open interval $(0, 1)$ are

$$\{V_k = X_k/d|\ \ k = 0, 1, 2, \cdots, \quad 0 < V_k < 1\},$$

which are to be regarded as a sample sequence of uniformly (and, hopefully independently) distributed random numbers to be used abundantly for computer simulations and for games. In order to press discussions to proceed smoothly, we supplement a few technical terms. Two integers A and B are said to be *equivalent modulo* d if

$$A - B = \alpha d, \quad \text{or} \quad B = A + \beta d$$

hold true. Hereafter Greek letters $\alpha, \beta, \cdots$ are taken to be *some* integers, the same letters of which can be different when used in different places. The function $\mathrm{mod}(A,\, d)$ with values kept in the interval $[0,\, d)$ may be stated to satisfy the *equation*

$$\mathrm{mod}(A,\, d) = A + \gamma d, \quad \text{with some integer } \gamma,$$

where the function $\mathrm{mod}(A,\, d)$ for a non-negative integer A is well known in computing languages. Soon we shall define $\mathrm{mod}(A,\, d)$ without ambiguity. As conceptual tecniques these saying will be seen to greatly simplify our understanding in proofs when used with $\mathrm{mod}(A,\, d)$. After all, please think that we cannot evade the use of the function $\mathrm{mod}(A,\, d)$ in numerical procedures.

[0003] In designing a random number generator we should mobilize all of our efforts to test out and find an excellent MC generator (d, z, n) that gives a random number sequence with an outstandding disguise for uniform and independent statistics. Though this subject of tests is vital in random number problems, the present invention is concerned with another significant feature in the generation of random numbers themselves. The resolution of the problem stems from the structures of the so-called Sunzi theorem, which relates numbers among themselves in notoriously abstruse fashion. We begin the discussion noting the origin of the need for Sunzi theorem. The first problem to be considered in the design of an MC (d, z, n) random number generator is the period T of the resultant MC sequence. Among many possibilities the basic structure is given by an odd prime modulus $d = p$ combined with its primitive root multiplier z, for which the little theorem of Fermat proves the period to be $T = p - 1$. However, we recognize that $p - 1$ is even, that $z^{(p-1)/2}$ is

equivalent to -1 modulo p, and that the second half of the cyclic sequence is just the negative of the first half. The second half cannot be used for *independent* random numbers. We thus define *the usable period* $T = (p-1)/2$ with the ratio $T/d \approx 1/2$. Hereafter we always use T for this *usable period*. In all cases of MC generators, the ratio T/d of the usable period to the modulus does not exceed $1/2$. We wish the longest possible *usable* period for any simulations. So, we start considerations from a prime-primitive root generator.

[0004] (Inadequacy of prime-primitive root generators) Let $d = p$ be an odd prime, and z be its primitive root giving the usable period $T = (p-1)/2$. In present times simulations are demanded of the usable periods $T \approx d/2$ to be not less than 2^{40}, say. Then we have the circumstance that zX_k in

$$X_0 = \mathrm{mod}(n,\ d), \quad X_{k+1} = \mathrm{mod}(zX_k,\ d), \quad k = 0, 1, 2, \cdots,$$

exceed the double precision *integer* limit 2^{64}. We should treat them as quadratic precision integers. Since such large integer arithmetic is absent in usual computers, we are forced to transform them to quadratic precision reals, perform the arithmetic, and then transform back to double precision integers securing the *reproducibility and transportability* of MC random numbers. The stated circuitous procedure is certainly possible, but takes 10 times or larger computing time, compared to the method we disclose here. This circumstance necessitates us to abandon the method to use single prime modulus with its primitive root multiplier. In fact we have found a prime $p \approx 2^{40}$ with an excellent primitive root multiplier Yet the stated circumstance force us the route. We in fact found a statistically excellent prime-primitive root (p, z, n) generator with the prime modulus $p \approx 2^{41}$. Yet this gives only the usable period of 2^{40}, which is too short for realistic simulations. Please *feel* the necessity to abandon the modulus design formed by a single prime.

[0005] (Sunzi theorem) Hereafter we assume the modulus d formed by a product of two *odd* distinct primes[2] $e_1 > 2$ and $e_2 > 2$ as $d = e_1 e_2$. There can be many forms of Sunzi theorem. We go directly into the one we use for the generation of MC (d, z, n) random numbers with the modulus $d = e_1 e_2$ formed by coprime odd positive submoduluses. Let us be explicit, rather than general. We assume that the modulus d is formed by 2 different odd primes $e_1 > 2$ and $e_2 > 2$.

Theorem 1 (Sunzi theorem) Suppose that the integer $d > 0$ for the modulus is a product $d = e_1 e_2$ of 2 distinct odd primes. [3] Let A be any non-negative integer. There holds the modular equation of A

[2] Please allow us to choose *distinct primes* or *coprime odd integers*, according to our ad hoc mood.
[3] Thus, the the greatest common divisor $\mathrm{GCD}(e_1,\ e_2) = 1$.

$$
\begin{aligned}
A &= \mathrm{mod}(A_1 D_1 D_1^{-1} + A_2 D_2 D_2^{-1},\, d) \qquad (*)\\
A_k &= \mathrm{mod}(A, e_k), \quad k = 1, 2,\\
D_k &= d/e_k, \;\; D_k^{-1} \text{is the inverse of } D_k \text{ modulo } e_k,\\
&\qquad\qquad \text{with } \mathrm{mod}(D_k D_k^{-1}, e_j) = \delta_{jk},\; j, k = 1, 2,
\end{aligned}
$$

We call $(*)$ as the *Sunzi decomposition* of the non-negative integer A, and prove after a few preliminary Corollaries and Lemmas. **(End of Theorem 1)**

[0006] The proof of **Theorem 1**is intricate, not to say difficult. In order to make it smooth, we prepare **Corollaries**.

Corollary 2 Let B be a non-negative integer. There holds

$$\mathrm{mod}(B,\, e) = B - \alpha e,$$

As stated, α is some integer and $e > 2$ is any of $e_1, e_2, d = e_1 e_2$.

(Proof) The $\mathrm{mod}(B,\, e)$ function brings the integer B to the interval $[0, e)$ by subracting or adding some integral multiple of e. Corollary is just, as it should. ■

Corollary 3 There holds

$$\mathrm{mod}(D_i D i^{-1},\, e_j) = \delta_{ij}.$$

Here δ_{ij} is Kronecker's delta which is 1 for $i = j$ and 0 otherwise.

(Proof) We have $D_1 = d/e_1 = e_2$ and $D_2 = d/e_2 = e_1$. Thus

$$
\begin{aligned}
&\mathrm{mod}(D_1 {D_1}^{-1},\, e_2) = \mathrm{mod}(e_2 {D_1}^{-1},\, e_2) = 0, \;\; \text{and}\\
&\mathrm{mod}(D_2 {D_2}^{-1},\, e_1) = \mathrm{mod}(e_1 {D_2}^{-1},\, e_1) = 0,
\end{aligned}
$$

are true. For other cases we have

$$
\begin{aligned}
&\mathrm{mod}(D_1 {D_1}^{-1}, e_1) = \mathrm{mod}(e_2 {e_2}^{-1}, e_1) = 1,\\
&\mathrm{mod}(D_2 {D_2}^{-1}, e_2) = \mathrm{mod}(e_1 {e_1}^{-1}, e_2) = 1,
\end{aligned}
$$

by definitions of ${D_1}^{-1}$ and ${D_2}^{-1}$. ■

Corollary 4 Let A, B be non-negative integers. Denote $A' = \mathrm{mod}(A,\, e)$ and $B' = \mathrm{mod}(B,\, e)$ where e is any of e_1 or e_2. There hold

(1) $\mathrm{mod}(A + B,\, e) = \mathrm{mod}(A' + B',\, e)$,

(2) $\mathrm{mod}(AB,\, e) = \mathrm{mod}(A'B',\, e)$.

(Proof) (1) We may write $A = \mathrm{mod}(A,\, e) + \alpha e = A' + \alpha e$ with some integer α. Likewise there holds $B = \mathrm{mod}(B,\, e) + \beta e = B' + \beta e$ with some integer β. Hence we

have

$$\begin{aligned}\mathrm{mod}(A+B,\,e) &= \mathrm{mod}(A'+\alpha e+B'+\beta e,\,e)\\ &= \mathrm{mod}(A'+B',\,e).\end{aligned}$$

The final outer mod cannot be dispensed with as non-negative integer $A'+B'$ may exceed $e>0$.

(2) There hold

$$\begin{aligned}\mathrm{mod}(AB,\,e) &= \mathrm{mod}(\{A'+\alpha e\}\{B'+\beta e\},e)\\ &= \mathrm{mod}(\{A'B'+\gamma e\},\,e) = \mathrm{mod}(A'B',\,e)\end{aligned}$$

with some integer γ. The final mod cannot be deleted, as $A'B'$ may exceed e. ■

[0007] (Proof of Theorem 1) We first note that as $\mathrm{GCD}(e_1,\,e_2)=1$ holds, Euclid algorithm proves the existence of integers M, N that give the *equation*

$$Me_1+Ne_2=1,\quad Me_1=1-Ne_2.$$

This implies

$$Me_1=1\ \bmod(e_2).$$

In other words, there is an inverse M' of $e_1\ \bmod(e_2)$ with $0<M'<e_2$.[4] Now we take an arbitrary non-negative integer A, compute $A_i=\mathrm{mod}(A,\,e_i)$ for $i=1,2$, and *construct the integer B defined by the r.h.s. of* $(*)$.[5] We have by the structure $d=e_1e_2$ and by **Corollary 2** and **Corollary 3**,

$$\mathrm{mod}(B,\,e_1)=\mathrm{mod}(\{\mathrm{mod}(A_1D_1{D_1}^{-1}+A_2D_2{D_2}^{-1},\,d)\},\,e_1).$$

We replace mod functions by equations of division. With the modulus e for any of d,e_1,e_2 and for any non-begative integer C, we may rewrite the function $\mathrm{mod}(C,\,e)$ as $\mathrm{mod}(C,\,e)=C+\alpha e$. Noting $D_2=e_1$, we have

$$\begin{aligned}&\mathrm{mod}(B,\,e_1)=B+\alpha e_1\\ &\quad=\mathrm{mod}(\{\mathrm{mod}(A_1D_1{D_1}^{-1}+A_2D_2{D_2}^{-1}\},\,d),\,e_1)\\ &\quad=\mathrm{mod}(\{\mathrm{mod}(A_1D_1{D_1}^{-1}+A_2D_2{D_2}^{-1}\},\,d),\,e_1)\\ &\quad=\mathrm{mod}(A_1D_1{D_1}^{-1}+\beta d,\,e_1)\\ &\quad=\mathrm{mod}(A_1,\,e_1)=A_1+\gamma e_1\\ &\quad=\mathrm{mod}(A,\,e_1)+\gamma e_1=A+\delta e_1.\end{aligned}$$

[4]The inverse M' of e_1 modulo e_2 is obtained by taking an integer x in $1,2,\cdots,e_2-1$, computing the product xe_1, and finding an integer x that gives $xe_1=1\ \bmod(e_2)$.

[5]Though we shall figure out that $B=A$, we denote temporarily B to erase any doubt.

This proves that $B-A$ is a multile of e_1. All the same, we have that $B-A$ is a multiple of e_2, coprime to e_1. Hence $B-A$ is a multiple of $d=e_1e_2$, or $B-A$ is some multiple of d. As both of A, B are in the interval $[0, d)$, there can only be $A=B$. This is a form of Sunzi theorem. ■

[0008] A different, abstract expression of **Theorem 1** will be helpful.
Corollary 5. (Sunzi Theorem) If the modulus $d>0$ is a product $d=e_1e_2$ of positive coprime integers e_1 and e_2, then any non-negative integer $A<d$ is expressed in a linear combination (or a *shuffling*) of integers

$$A_1=\mathrm{mod}(A, e_1), \quad A_2=\mathrm{mod}(A, e_2)$$

modulo-d uniquely as

$$A=\mathrm{mod}(\{A_1D_1{D_1}^{-1}+A_2D_2{D_2}^{-1}\}, d).$$

In words, we may state that the value A_1 of A modulo e_1 and the value A_2 of A modulo e_2 determine A uniquely modulo $d=e_1e_2$, if e_1 and e_2 are positive and coprime.

[0009] (An example from the MC generator #0001) Corollay 5 proved above may be felt perplexing, not to say magical. We shake off any doubt, by an example. Let $d=e_1e_2$ be the modulus of #001 with odd primes

$$e_1=134265023, \quad e_2=134475827.$$

The integer $A=1000000000000$ is decomposed modulo $d, e_1.e_2$ as follows:

$$\begin{gathered} A_1=128373719, \quad A_2=37750428, \\ D_1=e_2=134475827. \quad D_2=e_1=134265023. \\ {D_1}^{-1}=52577007, \quad {D_2}^{-1}=81816271, \\ A=\mathrm{mod}(A_1D_1{D_1}^{-1}+A_2D_2{D_2}^{-1}, d). \quad (*) \end{gathered}$$

The quoted $D_1, D_2, {D_1}^{-1}, {D_2}^{-1}$ are those for the excellent MC generator #0001 with the composite modulus $d=e_1e_2$. Please examine that the conclusion for the arbitrarily chosen integer A is correctly reproduced by the $(*)$ on your computer, with CALC as an exanmple.

[0010] Take the modulus $d=e_1e_2$ formed by a product of positive coprime integers $e_1.e_2$. Our aim is to discuss the Sunzi decomposition $(*)$ of the MC sequence according to the stated structure of the modulus, and see the effect given on computing structures found by Naoya Nakazawa. To this end we need to decompose

the general j-th term $A = \mathrm{mod}(nz^j,\, d)$ by submoduluses e_1, e_2. This is done as follows. We may use the expression of $A_k = \mathrm{mod}(A,\, e_k)$ (abbreviating the time variable j) for $k = 1, 2$ as follows:

$$\begin{aligned} A_k &= \mathrm{mod}(A,\, e_k) = \mathrm{mod}(\{\mathrm{mod}(nz^j.d)\},\, e_k) \\ &= \mathrm{mod}(\{nz^j + \alpha d\},\, e_k) \\ &= \mathrm{mod}(nz^j,\, e_k) = \mathrm{mod}(\{n_k + \beta e_k\}\{{z_k}^j + \gamma e_k\},\, e_k) \\ &= \mathrm{mod}(\{n_k {z_k}^j + \delta e_k\},\, e_k) \\ &= \mathrm{mod}(n_k {z_k}^j,\, e_k). \end{aligned}$$

This final form says that we need to consider only the Sunzi decomposition

$$A = \mathrm{mod}(nz^j,\, d) = \mathrm{mod}(n_1 {z_1}^j D_1 {D_1}^{-1} + n_2 {z_2}^j D_2 {D_2}^{-1},\, d).$$

with $j = 0, 1.2.\cdots$. As **Corollary 5** states, this result shows that the j-th MC output integer sequence $\mathrm{mod}(nz^j,\, d)$ is a simple suffling or a linear combination of j-th elements of integer sub-sequences,

$$\mathrm{mod}(n_1 {z_1}^j,\, e_1) \;\text{ and }\; \mathrm{mod}\,(n_2 {z_2}^j,\, e_2)$$

with coefficients $D_1 {D_1}^{-1}$ and $D_2 {D_2}^{-1}$ that do not depend on j in the mod function mdulo d. Thus, the j-th term V_j of the uniform MC random numbers in $(0, 1)$, is obtained by dividing this term in the integer sequence by the modulus d,

$$V_j = \mathrm{mod}(n_1 {z_1}^j D_1 {D_1}^{-1} + n_2 {z_2}^j D_2 {D_2}^{-1},\, d)/d.$$

with $j = 0, 1, 2, \cdots$. The outer $\mathrm{mod}(\cdots, d)$ cannot be dispensed with because the inner $\mathrm{mod}(n_1 {z_1}^j,\, e_1) D_1 {D_1}^{-1} + \mathrm{mod}(n_2 {z_2}^j,\, e_2) D_2 {D_2}^{-1}$ may exceed $d = e_2 e_2$.

[0011] We now show a direct computing program of (d, z, n) MC generator by the case of #001, The basic process is as usual. For the time development we may the recursive equations as well; please see the computing program shown below.
The computing program for these outputs has a standard and simple forms, as shown in **Figure 1** below. However, the computing speed for practical MC generators #001 is slow. Please see the notes further below.

A direct FORTRAN program

```
program main
implicit integer*8(i-p), real*8(a-h,r-z), real*16(q)
p1=134265023
p2=134475827
id=p1*p2                    ! d is approximately 2^54
qd=id
iz=7759097958782935d0
n=14899790517668688d0       ! the same initial data as Figure 2.
qmz=n
qz=iz
do i=1, 10000000
rand=mod(qmz,qd)/qd
qmz=mod(qmz*qz,qd)
end do
end
```

(End of Figure 1)

(Notes) The program needs 2.75sec CPU time for this 10^7 outputs. Compare the CPU time of 0.25sec obtained by the coming program that uses Sunzi reduction for the same number of outputs.

[0012] We recall that the Sunzi theorem was described on an arbitrary non-negative integer A and under a composite modulus $d = e_1 e_2$ formed by mutually coprime positive submoduluses e_1 and e_2. The Conclusion was the following *Sunzi decomposition*:

$$\begin{aligned} A &= \mathrm{mod}(A_1 D_1 D_1^{-1} + A_2 D_2 D_2^{-1},\, d) \qquad (*) \\ A_k &= \mathrm{mod}(A, e_k), \quad k = 1, 2, \\ D_k &= d/e_k, \;\; D_k^{-1} \text{is the inverse of } D_k \text{ modulo } e_k, \\ &\qquad \text{with } \mathrm{mod}(D_k D_k^{-1}, e_j) = \delta_{jk}, \;\; j, k = 1, 2, \end{aligned}$$

This magical relation is used now to obtain the step j MC integer output, by taking the integer A as follows.

$$A = \mathrm{mod}(nz^j,\, d), \quad j = 0, 1, 2, \cdots.$$

The necessary procedures for this application of $(*)$ are as follows.

(1) To compute the $A_k = \mathrm{mod}(A,\, e_k)$ for $k = 1, 2$:

(2) Calculate $A_k = \mathrm{mod}(A,\, e_k)$ for $k = 1, 2$:

(3) To compute $(*)$.

Now comes **(1)**. We define for $k = 1, 2$, leaving $j = 0, 1, 2, \cdots$ unspecified,

$$A_k = \mathrm{mod}(A,\, e_k) = \mathrm{mod}(\{\mathrm{mod}(nz^j,\, d)\},\, e_k).$$

We need definitions with some integers α, β,[6]

$$n_k = \mathrm{mod}(n,\, e_k) = n - \alpha e_k, \quad z_k = \mathrm{mod}(z,\, e_k) = z - \beta e_k, \;\; k = 1, 2.$$

These preparations give for the j-th output of the MC sequence

$$\begin{aligned} \mathrm{mod}(\mathrm{mod}(nz^j,\, d),\, e_k) &= \mathrm{mod}(nz^j + \gamma d,\, e_k) \\ &= \mathrm{mod}(\{n_k + \delta e_k\}\{{z_k}^j + \epsilon e_k\},\, e_k) \\ &= \mathrm{mod}(n_k {z_k}^j,\, e_k). \end{aligned}$$

This is a very plain and understandable result: In modulo e_k the MC seq uence $\mathrm{mod}(mz^j,\, d)$ looks as the j-th output of the subgenerator (e_k, z_k, n_k). In other words, we have

$$A_k = \mathrm{mod}(n_k {z_k}^j,\, e_K), \quad k = 1, 2$$

Thus for the j-th output of the MC (d, z, n) generator. we have very clear **(2)** and **(3)**,

$$A = \mathrm{mod}(nz^j,\, d) = \mathrm{mod}(n_1 {z_1}^j D_1 {D_1}^{-1} + n_2 {z_2}^j D_2 {D_2}^{-1}.\, d). \quad (**)$$

[0013] We go straight to the computing procedure using the above $(**)$, under an added restriction. *Hereafter we assume that* $2d = 2e_1e_2$ *does not exceed the double precision integer limit* 2^{64}. This is obeyed by MC random number generators #001 and #003 which are in our hand at present. The restriction enables us to proceed only with the double precision integer arithmetic and with the double precision real arithmetic, respecting the reproducitility and the transportability of the resultant MC generators. Please see the next page. The computing speed in this Sunzi reduced form is then about 0.281sec CPU time for this 10^7 outputs, about 10 times faster than Figure 1. This brilliant computing procedure was found by Naoya Nakazawa of HRF.

[6]Greek letters refer to integers. Please understand that the same Greek letter used before may refer to a different integer.

Figure 2: The main program to compute #001 MC sequence

```
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 ≈ 2^54
ad=id
iz1=19061252
iz2=77600525
n1=10                         ! seed1 is 10
n2=13                         ! seed2 is 13
ip2mp1=52577007
ip1mp2=81816271
mz1=mod(n1,ip1)
mz2=mod(n2,ip2)
do i=1,10000000
call random(rand)
end do
end
```

(Figure 2 end)

Figure 3: Subroutine program for #001

```
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=ip2*mz1a+ip1*mz2a
rand=az/ad
rand=mod(rand,1d0)
return
end
```

(Figure 3 end)

The CPU time of the above main program and subprogram based on Sunzi decomposition is $0.25\text{sec}/10^7$. This is 10 times faster than the direct computation using quadratic precision reals. We may strongly recommend:

Do use Sunzi reduction for all practical aims!