

Pseudo Random Numbers Generated By Using Mixture Of Modular Function And Tent Map

Epimaco A. Cabanlit, Jr.* and Mary Ann M. Vinson-Unggol

Mathematics Department, Mindanao State University, General Santos City, Philippines

*Corresponding author details: Epimaco A. Cabanlit, Jr.; maco_727@yahoo.com

ABSTRACT

In this paper, we develop an algorithm in generating random numbers from the mixture of the modular function and the tent map. Results show that there are more random numbers generated from the mixture compared to the random numbers generated purely from the modular function and the tent map. Moreover, majority of the distributions of the generated random numbers for the mod100 are uniform. However, the distributions of the generated random numbers for the mod1000 are not uniform. Lastly, the sequences of random numbers generated for divisor of mod100 and mod1000 behave to be random.

Keywords: random numbers; modular function; tent map; algorithm

INTRODUCTION

The use of random numbers in statistics has extended more than in random sampling and random assignment of treatments to experimental units [1]. They are now being used in simulation studies such as in stochastic processes, engineering, biological sciences and cryptography. In cryptography, the requirements for “randomness” are more stringent than for ordinary applications in simulation [1].

Things that make random numbers are generically called Random Number Generators (RNGs), and they are classified into two major types: Pseudo-Random Numbers Generators (PRNGs) and True Random Number Generators (TRNGs). PRNGs are deterministic algorithms, while TRNGs are nondeterministic systems [2].

The digital computer cannot generate true random numbers, and it is not convenient to connect the computer to some external source of random events [1]. However, this can be overcome if there are some sources of pseudorandom numbers in which samples can be drawn from some known distributions.

True random numbers have some disadvantages, among them are: 1. The random numbers are to be extracted from natural resources which demand a lot of hardware and are expensive to set up. 2. The generation speed of random numbers may not be sufficient for the application. 3. Entropy sources can be influenced by the changes in the physical environment of the device like changes in the temperature, changes in the voltage or frequency of the power supply, exposure to radiation, etc.. 4. An intruder can control some of the parameters that may affect the entropy value [4].

It can be noted that one of the most important methodologies in operations research, numerical analysis and statistics is the deployment of random experiments for solving problems [3]. The method of random experiments has undergone since the end of 1940's, a fast development for in those years the rapid growth in the computational capacities of the computers made the executions of the random experiments in really large numbers possible [3].

As of this time, there are many pseudo random numbers generators being developed: Some are Middle Square Method, Linear Feedback Shift Registers and Xorshift Generators [4]. The extraction of the numbers in the square root of 2 is also a potential can be a good method of generating random numbers [5].

Recently, Padua [6] hinted that the tent map can generate U(0,1) variates and the logistic map can be a good substitute for the arcsine law.

Modular arithmetic can be handled mathematically by introducing a congruence relation on the integers that is compatible with the operations of the ring of integers: addition, subtraction, and multiplication. For a fixed modulus n , it is defined as follows. Two integers a and b are said to be congruent modulo n , if their difference $(a-b)$ is an integer multiple of n . If this is the case, it is expressed as: $a \equiv b \pmod{n}$. [7]

On the other hand, the tent map, formed by the iteration of the output value in a transformation of modular function, can be used for the generation of random numbers, given by the equation

$$T(x) = \begin{cases} 2x, & \text{for } 0 \leq x < \frac{1}{2} \\ 2 - 2x, & \text{for } \frac{1}{2} \leq x < 1 \end{cases}$$

In this paper, we present an algorithm in generating random pseudo numbers by using the mixture of modular function and tent map that can automatically create long runs of numbers.

THE ALGORITHMS

This paper ventures to generate random numbers by getting the mixture of the modular and tent map. Important developments, results and findings of the study are the following:

(1) Algorithm for Modular Function. These are the following steps in generating random numbers by using the Modular:

1. Input $X_n, n = 0$.
2. Compute $X_{n+1} = (X_n \cdot (P_1 + P_2)) \bmod N$

(2) Algorithm for Tent Map. These are the following steps in generating random numbers by using the Tent Map:

1. Input $X_n, n = 0$.
2. Let $X_n = Y_n$.
3. Convert Y_n to a number from 0 to 1 by dividing it by N, where N is the number of digits from the decimal point of X_n .

4. Compute
$$Y_{n+1} = \begin{cases} 2Y_n, & \text{for } 0 \leq Y_n < \frac{1}{2} \\ 2 - 2Y_n, & \text{for } \frac{1}{2} \leq Y_n < 1 \end{cases}$$

5. Convert Y_{n+1} to a whole number by multiplying it by N.

(3) Algorithm for Mixtures of Modular and Tent Map. These are the following steps in generating random numbers by using the mixtures of Modular and Tent map:

1. Input $X_n, n = 0$.
2. Compute $X_{n+1} = (X_n \cdot P_1 + P_2) \bmod N$.
3. Let $X_n = Y_n, n = 0$.
4. Convert Y_n to number from 0 to 1 by dividing it

by N. That is,
$$W_n = \frac{Y_n}{N}$$

5. Compute
$$W_{n+1} = \begin{cases} 2W_n, & \text{for } 0 \leq W_n < \frac{1}{2} \\ 2 - 2W_n, & \text{for } \frac{1}{2} \leq W_n < 1 \end{cases}$$

6. Convert W_{n+1} to a whole number by multiplying it by N. That is, $Z_{n+1} = NW_{n+1}$

7. Compute $\frac{X_{n+1} + Z_{n+1}}{2}$. This is the random number generated.

8. Go to step 2 for the computation of X_{n+1} . Go to step 4 for the computation of Z_{n+1} .

We consider the following as examples:

$P_1 = 263, P_2 = 71, X_0 = 79.49, 33, 85.66$ for $N = 100$
and $X_0 = 799.499, 330, 850.660$ for $N = 1000$.

THE RESULTS

Tables 1 and 2 give a brief summary of the characteristics of the random numbers generated.

TABLE 1: Characteristics of the Random Numbers Generated N=100.

Seeds X_0		33	49	66	79	85
Number of Random Numbers Generated	Modular	20	20	20	20	20
	Tent Map	12	12	11	12	12
	Mixtures of Modular and Tent Map	22	22	21	22	22
Test for Uniformity		$\chi^2 = 2.5^*$	$\chi^2 = 12.5$	$\chi^2 = 4^*$	$\chi^2 = 5^*$	$\chi^2 = 4^*$
Test for Randomness		$z = 0.42^{**}$	$z = -1.35^{**}$	$z = -0.42^{**}$	$z = 0.46^{**}$	$z = 0.47^{**}$

*-Distribution is uniform

** - Sequence of numbers vary randomly

Table 1 shows the characteristics of the random numbers generated by Modular, Tent Map, and the Mixture of the Modular and Tent Map where $N=100$. It can be observed that there are more random numbers generated by the mixture of the Modular and Tent Map compared to the Modular and Tent Map.

χ^2 values show that majority of the distributions of the random numbers generated are uniform. Z-values also show that the sequence of numbers generated varies randomly at 0.05 probability level.

TABLE 2: Characteristics of the Random Numbers Generated N=1000.

Seeds X_0		330	490	660	790	850
Number of Random Numbers Generated	Modular	100	100	100	100	100
	Tent Map	12	12	11	12	12
	Mixtures of Modular and Tent Map	102	102	101	102	102
Test for Uniformity		$\chi^2 = 36.5$	$\chi^2 = 31.7$	$\chi^2 34.8$	$\chi^2 = 27.3$	$\chi^2 = 36.5$
Test for Randomness		$z = -0.79^{**}$	$z = 0.197^{**}$	$z = 0.8^{**}$	$z = -0.99^{**}$	$z = 0.99^{**}$

*-Distribution is uniform

** - Sequence of numbers vary randomly

Table 2 shows the characteristics of the random numbers generated by Modular, Tent Map, and the Mixture of the Modular and Tent Map where $N=1000$. It can be observed that there are more random numbers generated by the mixture of the Modular and Tent Map compared to the Modular and Tent Map. χ^2 values show that the distributions of the random numbers generated are not uniform. Z-values also show that the sequence of numbers generated varies randomly at 0.05 probability level.

CONCLUDING REMARKS

This study has a very interesting results where we can get more random numbers generated by the Mixture of the Modular and Tent Map compared to the Modular and Tent Map. Majority of the distribution of the generated random numbers for $N = 100$ is uniform. However, the distribution of the generated random numbers for $N = 1000$ is not uniform. The sequence of random numbers generated for $N = 100$ and $N = 1000$ behaves to be random. Hence, we recommend further study on generating random numbers particularly on the mixture of modular and chaotic functions and an investigation of the distribution of the random numbers generated by the mixture of modular and tent map.

REFERENCES

[1] Gentle, James E. Random Number Generation and Monte Carlo Methods, 2nd ed. Springer Science-Business Media, New York, 2003.

[2] Johnston, David. Random Number Generators-Principles and Practices. Walter de Guyter GmbH, Berlin/Boston, 2018.

[3] Deak, Istvan. Random Number Generators and Simulation. Akademia Kiado, Budapest. 1990.

[4] Thomas, Antu Annam and Paul, Varghese. Nested Random Generator. International Journal of Advanced Research in Computer Science and Software Engineering. Volume 2, Issue 5, May 2017. pp767-773.

[5] Cabanlit, Epimaco, Jr. A and Bingco. Bethany Love E. Distribution and Randomness of the Numbers in $\sqrt{2}$. International Journal of Scientific Advances. Volume 3, Issue 4. July-August, 2022. pp. 588-590. DOI: 10.51542/ijscia.v3i4.21.

[6] Padua, R.N. Statistical Viewpoint for Chaos and Dynamical System. Journal of Mathematical Sciences, Vol 2, No. 1, 1999. Mindanao Polytechnic State College, Cagayan de Oro City, Philippines.

[7] Mulatu Lemma and Dustin Allard. Applications of Congruence to Divisibility Theory. IJRDO-Journal of Mathematics. Volume-3 | Issue-11 | November,2017. PP 4-5.

APPENDIX A (Random Numbers Generated)

Seed value =79			Seed value=49		
Modular	Chaos	Mixture	Modular	Chaos	Mixture
48	42	45	58	98	78
95	84	90	25	4	15
56	32	44	46	8	27
99	64	82	69	16	43
8	72	40	18	32	25
75	56	66	5	64	35
96	88	92	86	72	79
19	24	22	89	56	73
68	48	58	78	88	83
55	96	76	85	24	55
36	8	22	26	48	37
39	16	28	9	96	53
28	32	30	38	8	23
35	64	49	65	16	41
76	72	74	66	32	49
59	56	57	29	64	47
88	88	88	98	72	85
15	24	19	45	56	51
16	48	32	6	88	47
79	96	87	49	24	37
48	8	28	58	48	53
95	16	56	25	96	61
56	32	44	46	8	27
99	64	82	69	16	43
8	72	40	18	32	25

Seed Value=33			Seed value=85		
Modular	Chaos	Mixture	Modular	Chaos	Mixture
50	66	58	26	26	26
21	68	45	9	52	31
94	64	79	38	96	67
93	72	83	65	8	37
30	56	43	66	16	41
61	88	75	29	32	31
14	24	19	98	64	81
53	48	51	45	72	59
10	96	53	6	56	31
1	8	5	49	88	69
34	16	25	58	24	41
13	32	23	25	48	37
90	64	77	46	96	71
41	72	57	69	8	39
54	56	55	18	16	17
73	88	81	5	32	19
70	24	47	86	64	75
81	48	65	89	72	81
74	96	85	78	56	67
33	8	21	85	88	87
50	16	33	26	24	25
21	32	27	9	48	29
94	64	79	38	96	67
93	72	83	65	8	37
30	56	43	66	16	41

Seed value=66			Seed value=790		
Modular	Chaos	Mixture	Modular	Chaos	Mixture
29	68	49	841	420	631
98	64	81	254	840	547
45	72	59	873	320	597
6	56	31	670	640	655
49	88	69	281	720	501
58	24	41	974	560	767
25	48	37	233	880	557
46	96	71	350	240	295
69	8	39	121	480	301
18	16	17	894	960	927
5	32	19	193	80	136
86	64	75	830	160	495
89	72	81	361	320	341
78	56	67	14	640	327
85	88	87	753	720	737
26	24	25	110	560	335
9	48	29	1	880	441
38	96	67	334	240	287
65	8	37	913	480	697

66	16	41	190	960	575
29	32	31	41	80	61
98	64	81	854	160	507
45	72	59	673	320	497
6	56	31	70	640	355
			481	720	601
			574	560	567
			33	880	457
			750	240	495
			321	480	401
			494	960	727
			993	80	537
			230	160	195
			561	320	441
			614	640	627
			553	720	637
			510	560	535
			201	880	541
			934	240	587
			713	480	597
			590	960	775
			241	80	161
			454	160	307
			473	320	397
			470	640	555
			681	720	701
			174	560	367
			833	880	857
			150	240	195
			521	480	501
			94	960	527
			793	80	437
			630	160	395
			761	320	541
			214	640	427
			353	720	537
			910	560	735
			401	880	641
			534	240	387
			513	480	497
			990	960	975
			441	80	261
			54	160	107
			273	320	297
			870	640	755
			881	720	801
			774	560	667
			633	880	757
			550	240	395

			721	480	601
			694	960	827
			593	80	337
			30	160	95
			961	320	641
			814	640	727
			153	720	437
			310	560	435
			601	880	741
			134	240	187
			313	480	397
			390	960	675
			641	80	361
			654	160	407
			73	320	197
			270	640	455
			81	720	401
			374	560	467
			433	880	657
			950	240	595
			921	480	701
			294	960	627
			393	80	237
			430	160	295
			161	320	241
			414	640	527
			953	720	837
			710	560	635
			801	880	841
			734	240	487
			113	480	297
			790	960	875
			841	80	461
			254	160	207
			873	320	597
			670	640	655
			281	720	501

Seed value =490			Seed value=330		
Modular	Chaos	Mixture	Modular	Chaos	Mixture
941	980	961	861	660	761
554	40	297	514	680	597
773	80	427	253	640	447
370	160	265	610	720	665
381	320	351	501	560	531
274	640	457	834	880	857
133	720	427	413	240	327
50	560	305	690	480	585

221	880	551	541	960	751
194	240	217	354	80	217
93	480	287	173	160	167
530	960	745	570	320	445
461	80	271	981	640	811
314	160	237	74	720	397
653	320	487	533	560	547
810	640	725	250	880	565
101	720	411	821	240	531
634	560	597	994	480	737
813	880	847	493	960	727
890	240	565	730	80	405
141	480	311	61	160	111
154	960	557	114	320	217
573	80	327	53	640	347
770	160	465	10	720	365
581	320	451	701	560	631
874	640	757	434	880	657
933	720	827	213	240	227
450	560	505	90	480	285
421	880	651	741	960	851
794	240	517	954	80	517
893	480	687	973	160	567
930	960	945	970	320	645
661	80	371	181	640	411
914	160	537	674	720	697
453	320	387	333	560	447
210	640	425	650	880	765
301	720	511	21	240	131
234	560	397	594	480	537
613	880	747	293	960	627
290	240	265	130	80	105
341	480	411	261	160	211
754	960	857	714	320	517
373	80	227	853	640	747
170	160	165	410	720	565
781	320	551	901	560	731
474	640	557	34	880	457
733	720	727	13	240	127
850	560	705	490	480	485
621	880	751	941	960	951
394	240	317	554	80	317
693	480	587	773	160	467
330	960	645	370	320	345
861	80	471	381	640	511
514	160	337	274	720	497
253	320	287	133	560	347
610	640	625	50	880	465
501	720	611	221	240	231

834	560	697	194	480	337
413	880	647	93	960	527
690	240	465	530	80	305
541	480	511	461	160	311
354	960	657	314	320	317
173	80	127	653	640	647
570	160	365	810	720	765
981	320	651	101	560	331
74	640	357	634	880	757
533	720	627	813	240	527
250	560	405	890	480	685
821	880	851	141	960	551
994	240	617	154	80	117
493	480	487	573	160	367
730	960	845	770	320	545
61	80	71	581	640	611
114	160	137	874	720	797
53	320	187	933	560	747
10	640	325	450	880	665
701	720	711	421	240	331
434	560	497	794	480	637
213	880	547	893	960	927
90	240	165	930	80	505
741	480	611	661	160	411
954	960	957	914	320	617
973	80	527	453	640	547
970	160	565	210	720	465
181	320	251	301	560	431
674	640	657	234	880	557
333	720	527	613	240	427
650	560	605	290	480	385
21	880	451	341	960	651
594	240	417	754	80	417
293	480	387	373	160	267
130	960	545	170	320	245
261	80	171	781	640	711
714	160	437	474	720	597
853	320	587	733	560	647
410	640	525	850	880	865
901	720	811	621	240	431
34	560	297	394	480	437
13	880	447	693	960	827
490	240	365	330	80	205
941	480	711	861	160	511
554	960	757	514	320	417
773	80	427	253	640	447
370	160	265	610	720	665
381	320	351	501	560	531

Seed value=850			Seed value=660		
Modular	Chaos	Mixture	Modular	Chaos	Mixture
621	260	441	651	680	
394	520	457	284	640	666
693	960	827	763	720	462
330	80	205	740	560	742
861	160	511	691	880	650
514	320	417	804	240	786
253	640	447	523	480	522
610	720	665	620	960	502
501	560	531	131	80	790
834	880	857	524	160	106
413	240	327	883	320	342
690	480	585	300	640	602
541	960	751	971	720	470
354	80	217	444	560	846
173	160	167	843	880	502
570	320	445	780	240	862
981	640	811	211	480	510
74	720	397	564	960	346
533	560	547	403	80	762
250	880	565	60	160	242
821	240	531	851	320	110
994	480	737	884	640	586
493	960	727	563	720	762
730	80	405	140	560	642
61	160	111	891	880	350
114	320	217	404	240	886
53	640	347	323	480	322
10	720	365	20	960	402
701	560	631	331	80	490
434	880	657	124	160	206
213	240	227	683	320	142
90	480	285	700	640	502
741	960	851	171	720	670
954	80	517	44	560	446
973	160	567	643	880	302
970	320	645	180	240	762
181	640	411	411	480	210
674	720	697	164	960	446
333	560	447	203	80	562
650	880	765	460	160	142
21	240	131	51	320	310
594	480	537	484	640	186
293	960	627	363	720	562
130	80	105	540	560	542
261	160	211	91	880	550
714	320	517	4	240	486
853	640	747	123	480	122

410	720	565	420	960	302
901	560	731	531	80	690
34	880	457	724	160	306
13	240	127	483	320	442
490	480	485	100	640	402
941	960	951	371	720	370
554	80	317	644	560	546
773	160	467	443	880	602
370	320	345	580	240	662
381	640	511	611	480	410
274	720	497	764	960	546
133	560	347	3	80	862
50	880	465	860	160	42
221	240	231	251	320	510
194	480	337	84	640	286
93	960	527	163	720	362
530	80	305	940	560	442
461	160	311	291	880	750
314	320	317	604	240	586
653	640	647	923	480	422
810	720	765	820	960	702
101	560	331	731	80	890
634	880	757	324	160	406
813	240	527	283	320	242
890	480	685	500	640	302
141	960	551	571	720	570
154	80	117	244	560	646
573	160	367	243	880	402
770	320	545	980	240	562
581	640	611	811	480	610
874	720	797	364	960	646
933	560	747	803	80	662
450	880	665	260	160	442
421	240	331	451	320	210
794	480	637	684	640	386
893	960	927	963	720	662
930	80	505	340	560	842
661	160	411	491	880	450
914	320	617	204	240	686
453	640	547	723	480	222
210	720	465	220	960	602
301	560	431	931	80	590
234	880	557	924	160	506
613	240	427	83	320	542
290	480	385	900	640	202
341	960	651	771	720	770
754	80	417	844	560	746
373	160	267	43	880	702
170	320	245	380	240	462

781	640	711	11	480	310
474	720	597	964	960	246
733	560	647	603	80	962
850	880	865	660	160	342
621	240	431	651	320	410
394	480	437	284	640	486
693	960	827	763	720	462
330	80	205	740	560	742
861	160	511	691	880	650