Fibonacci Random Number Generator using Lehmer's Algorithm

*1Oduwole, H. K., [1]Shehu, S. L., [1]Adegoke, G. K. & [1]Onubogu, J. L.

1. Department of Mathematical Sciences, Nasarawa State University, Keffi, Nasarawa State, Nigeria

* E-mail of the corresponding author: kenresearch@yahoo.com

Abstract

The uniqueness of Fibonacci sequence is been discussed with particular emphasis on its application to random number generation. The Lehmer's algorithm was employed using fibonacci prime. For multiplier $a = 912$, initial seed $x_0 = 415$, modulus $m = 28657$ and multiplier $a = 518$, initial seed $x_0 = 211$, modulus $m = 514229$, we generate random numbers with full period $(m-1)$. This suggest that higher values of Fibonacci primes with appropriate choice of a full multiplier a, modulus m (fibonacci prime) and a starting seed x_0 will produce a full period with finite countable many random numbers. A run test also indicates that the random numbers generated using modulus m as fibonacci prime are truly random

Keywords: Fibonacci sequence, Fibonacci prime, Random numbers generator, Lehmer's Algorithm, run test

1. Introduction

The design of nature has been discovered to have underlying mathematical formulation and numerical representations. One such numerical representation found in nature is Fibonacci numbers (Adam, 2006). The Fibonacci numbers are sequence of numbers generated by summing the first two numbers in the sequence to get the next. It is a deceptively simple series of numbers but it ramifications and applications are nearly limitless (Livio, 2002; Conway and Guy, 1996). The Fibonacci sequence is of interest to non-mathematicians primarily because of the possibility of using them to investigate a wide variety of problems. These numbers are researched in the area of number theory, games theory and sequence and it has continued to attract interest among mathematicians to the extent that a quarterly journal is dedicated to Fibonacci series (Hilton & Pedersen, 1994; Matthew & Fink, 2004).

A random number is a number generated by a process which outcome is unpredictable and which cannot be subsequently reliably reproduced. This definition works fine provided that one has some kind of black box, such a black box is usually called random number generator that fulfil the required task. (von Neumann, 1951) Consequently, a random number can also be defined as a number chosen by chance from some specified distribution such that selection of a large set of these numbers produces the underlying statistical distribution. Almost always such numbers are also required to be independent, so that there are no correlations between successive members. The output can be converted to random variate via mathematical transformations

Historically there are two types of random numbers generators: computer generators (also called True random number generator (TRNG) and algorithmic generators (also called Pseudo-random numbers generator (PRNG)). Pseudo random number generators are algorithm that uses mathematical formulae or simply pre-calculated table to produce sequence of number that appear random. A good deal of research has gone into pseudo random number theory and modern algorithms for generating pseudo random number and it makes it so good that the number look exactly like they were really random (Knuth, 1997). A good example of pseudo random number generators is the linear congruential method. A linear congruential generator is a method of generating a sequence of numbers that are not actually random but share many properties with complete random numbers. (Neave, 1973 ;Ferguson, 1960).

Pseudo-random numbers generators are widely accepted because they meet the following criteria: **randomness:** It produces output passes all reasonable statistical tests of randomness; **controllability:** able to reproduce random stream of output, if desired; **portability:** able to produce the same output on a wide variety of computer systems **efficiency:** fast, minimal computer resource requirements and **documentation:** theoretically analysed and extensively tested. When used without qualification the word random usually means random with a uniform distribution, other distribution are of course possible. For example the box-miller transformation allows pairs of uniform random numbers to be transformed to the corresponding random numbers having a two dimensional distribution. It is impossible to produce an arbitrary long string of digits and prove that it is random. When generating random numbers over some specified boundary, it is often necessary to normalize the distribution so that all differential areas are equally computed (Bassein, 1996).

True random number generators (TRNG) extract randomness from physical phenomenon and introduce it into the computer. The physical phenomenon can be very simple like the little variations in the movement of a mouse or in the amount of time between key strokes. Regardless of which physical phenomenon that is used, the process of generating true random number involves identifying little unpredictable changes in the real life data.

2. An Overview of Lehmer's Algorithms

Using the note of Leemis and Park, (2006) and Shorey and Stewart, (1981) we present some basic concepts on Lehmer's algorithm. Lehmer's algorithm for random number generation is defined in terms of two fixed parameters: **modulus** $\boldsymbol{m}$, a fixed large prime integer and **multiplier** $\boldsymbol{a}$, a fixed integer in X_m

The integer sequence $x_0, x_1, \cdots$ is defined by the iterative equation $x_{i+1} = g(x_i)$
with $g(x_i) = ax_i \bmod m$
$x_0 \in X_m$ is called the initial seed
We have that $0 \leq g(x_i) < m$ because of the mod operator.
However, 0 must not occur since $g(0) = 0$
Since m is prime, $g(x) \neq 0$ if $x \in X_m$.
If $x_0 \in X_m$, then $x_i \in X_m$ for all $i \geq 0$.

Note: The quality of Pseudo-Random numbers generated depends on a good choice of $\boldsymbol{a}$ (multiplier) and $\boldsymbol{m}$ (modulus). The following observations are important:

- a is a fixed (constant) integer in X_m also known as **multiplier**
- m is a large fixed prime integer also known as the **modulus**
- x_0 is the initial starting seed in X_m

- The **Mod** function ensures a value less than m is always generated,
- m (Modulus) is chosen to be a prime number so that a non-zero remainder always exist, that is x_i is never 0. If x_i becomes 0, then all subsequent x_i will be zero

2.1 The Modulus and Multiplier Selection

Here we discuss how to select a suitable modulus and multiplier that can generate the desired random numbers. When selecting a modulus or multiplier, the following outlined rules must be noted:

(i). The modulus m should be very large as possible ($2^{31} - 1$ is a good value for modulus m).

(ii). The modulus must be a prime number in other to avoid the occurrence of zero which subsequently causes x_i to be zero.

(iii). The multiplier a should be chosen to guarantee a full period multiplier.

Theorem 1

If the sequence $x_0, x_1, x_2, \cdots$ is a produce by Lehmer's generator with multiplier a and modulus m then $x_i = a^i x_0 \text{mod}\, m$

Proof

We know that $b \text{ mod } a = b - \left[{}^{b}/_{a}\right]a$, then there exist a non-negative integer $c_i = \left[{}^{ax_i}/_{m}\right]$ such that

$x_{i+1} = g(x_i) = ax_i \text{mod}\, m = ax_i - mc_i$

Therefore (by induction), we have that

$x_1 = ax_0 - mc_0$

$x_2 = ax_1 - mc_1 = a^2 x_0 - m(ac_0 + c_1)$

$x_3 = ax_2 - mc_2 = a^3 x_0 - m(a^2 c_0 + ac_1 + c_2)$

$\vdots \quad \vdots \qquad \vdots$

$x_i = ax_{i-1} - mc_{i-1} = a^i x_0 - m(a^{i-1} c_0 + a^{i-2} c_1 + \cdots + c_{i+1})$

since $x_i \in \chi_m$, we have that $x_i = x_i \text{mod}\, m$

Therefore letting $c = a^{i-1} c_0 + a^{i-2} c_1 + \cdots + c_{i+1}$, we have that

$x_i = a^i x_0 - mc = (a^i x_0 - mc) \text{mod}\, m = a^i x_0 \text{mod}\, m$

Hence $x_i = a^i x_0 \text{mod}\, m$

Note: We do not compute x_i by first computing a^i, this is a wrong approach.

The result of Theorem 1 has a significant theoretical value.

2.2 The Period of the Sequence

Consider sequence produced by $x_{i+1} = a \cdot x_i \text{mod}\, m$, once a value is repeated, all the sequence is then repeated. That is the sequence: $x_0, x_1, x_2, \cdots, x_i, \cdots, x_{i+p}$ where $x_i = x_{i+p}$. p is the period, that is the number of elements before the first repeat. Clearly we see that $p \leq m - 1$

It can be shown, that if we pick *any* initial seed x_0, we are guaranteed this initial seed will reappear.

Theorem 2

If $x_0 \in \chi_m$ and the sequence $x_0, x_1, x_2, \cdots$ is produced by the Lehmer's generator $x_{i+1} = a \cdot x_i \bmod m$ with multiplier a and (prime) modulus m, then there exist a positive integer p with $p \leq m-1$ such that:

(i). $x_0, x_1, \cdots, x_{p-1}$ are all different and

(ii). $x_{i+p} = x_i, \quad \forall\, i = 0, 1, 2, \cdots$

Proof

We know from modulo arithmetic that

$(b_1 . b_2 \ldots b_n) \bmod a = (b_1 . \bmod \mathrm{a})(b_2 . \bmod \mathrm{a}) \ldots (b_n . \bmod \mathrm{a})$

Therefore $x_i = a^i \cdot x_0 \bmod m = (a^i \bmod m) x_0 \bmod m$

From Fermat's Little theorem, which states that if p is a prime which does not divides a, then

$a^{p-1} \bmod p = 1$ … … … … (*.1)

Then x_{m-1}=$(a^{m-1} \bmod m) x_0 \bmod m = x_0$ … … … … (*.*)

From (*.*), we have a more defined generalization, thus x_{i+p}=$(a^{i+p} \bmod p) x_i \bmod m = x_i$

$\Longrightarrow x_{i+p}$= x_i Hence the proof

Note:

1. Ideally, the generator cycles through all values in χ_m to maximize the number of possible values that are generated, and guarantee any number can be produced.
2. The sequence containing all possible numbers is called a **full-period sequence** $(p = m-1)$.
3. Non-full period sequences effectively partition χ_m into disjoint sets, each set has a particular period (not full period).

2.3 Determining if a is a full period Multiplier

We present the following Algorithm for finding if p is a full period.

```
p = 1;
x = a;        // assume, initial seed is   x0 = 1, thus  x1 = a
Do
    x=(a * x)mod m          {// cycle through numbers until repeat//}
    p = p + 1       {careful: overflow possible}
Until   x = x0
If   p = m − 1
    Writeln (a  is a full period multiplier)
Else
        Writeln (a  is not a full period multiplier)
End if
```

3. Numerical Experiments

The following numerical experiments show how random numbers are generated using Lehmer's algorithm of the formula x_{i+1}=$a * x_i \bmod m$, considering the multiplier a, the modulus m and the initial seed x_0. In each experiment we generate values for $x_0, x_1, x_2, \cdots, x_i, x_{i+1}$ after making a choice of fibonacci prime as our values for m

Experiment 1 $(m = 28657, a = 912, x_0 = 415)$ – Five digit fibonacci prime (m)
Experiment 2 $(m = 514229, a = 518, x_0 = 211)$ – Six digit fibonacci prime (m)
The two numerical experiment above produce a full period sequence since $p = 28657$ (first experiment) and $p = 514229$ (second experiment) therefore $a = 912$ and $a = 518$ are full period multiplier respectively.

3.1 Tests for Randomness

We apply the run test to test the null hypothesis that randomness does not exist in the number generated. Consider a sequence of numbers made up of two set, c and d, where c represent the corresponding random numbers generated when it is less than the average and d represent the corresponding random numbers generated when it is greater than the average.
Suppose we form all possible sequences consisting of $N_1 c's$ and $N_2 d's$, for $N_1 + N_2 = N$ and V is the total number of runs, then by using the formula

$$\mu_v = \frac{2N_1N_2}{N_1+N_2} + 1 \qquad \dots \quad \dots \quad \dots \quad \dots \quad (1)$$

$$\delta_v^2 = \frac{2N_1N_2(2N_1N_2 - N_1 - N_2)}{(N_1+N_2)^2(N_1+N_2-1)} \qquad \dots \quad \dots \quad \dots \quad \dots \quad (2)$$

When N is relatively large (>20) the distribution of V is approximately normal and thus

$$Z = \frac{V-\mu_v}{\delta_v} \sim N(0,1) \qquad \dots \quad \dots \quad \dots \quad \dots \quad (3)$$

We can test the null hypothesis at the appropriate level of significance using equation (3)
We have that for the first experiment
$N_1 = 14329,\ N_2 = 14328,\ N = 28657,\ V = 14448.9$
We have that $\mu_v = 14329.5$ and $\delta_v = 84.6404$ and $Z_{cal} = 1.41076$, $Z_{Table} = 1.96$, for $\alpha = 0.05$ level of significance.
Therefore we reject the null hypothesis and conclude that randomness exist in the random numbers generated since Z_{cal}(Test statistics) $<$ Z_{Table} (Critical value)
Using the same approach above, for the second experiment we test for the null hypothesis and conclude that randomness exist in the sets of random number generated.

4 Results and Discussion

From the result of this work, we have shown that a five and six digit fibonacci prime with appropriate choice of full multiplier a, modulus m (fibonacci prime) and a starting seed x_0 will produce a full period. Table 1 shows the first 600 random numbers generated from the 28, 657 that was generated and Table 2 shows the first 570 random numbers generated from the 514, 229 that was generated. A full period guarantees randomness and a longer length of random numbers sets. The longer the digit of the fibonacci prime, the better and more random the numbers generated will be. Further research should be able to show clearly that not all fibonacci prime will generates a full period no matter the choice of full multiplier a, and a starting seed x_0.

Table 1: Showing the first 600 random numbers from the 28, 657 that was generated $(m = 28657, a = 912, x_0 = 415)$

415	27806	9479	4869	2238	2247	27571	984	8133	25721	7885	12488	8159	6540	13865	14036	8023	18696	11242	1530
5939	26284	19091	27350	6409	14617	12563	9041	23790	16126	26870	12227	18845	3824	7143	19810	9441	28494	22155	19824
195	13756	16193	11610	27637	5199	23313	20833	3131	5871	3705	3451	21097	19991	9277	12810	13092	23286	2175	25578
5898	22363	9661	13887	15441	13083	26619	105	18429	24150	26091	23699	11617	5940	6809	19321	18592	1995	6267	338
20117	19929	13133	27207	11605	10384	4049	9789	14246	16224	9682	6110	20271	1107	19896	25354	19617	14049	12761	21686
6224	6710	27327	24479	9327	13398	24592	15241	10731	9276	3628	12862	3387	6589	5271	25306	8736	3009	3290	4302
2202	15579	19291	1045	23752	11094	18130	1147	14635	5897	13181	9431	22645	19855	21433	10187	586	21793	20152	26072
2234	22833	26651	7359	25789	1807	28128	14412	21615	19205	13789	3972	19200	25193	2822	5676	18606	15915	9487	21011
2761	18714	4576	5670	20828	14535	4721	18838	25521	5533	23802	11682	973	21759	23191	18252	3728	14038	26387	19156
24873	16253	18047	12780	24202	16386	7002	14713	5668	2464	14075	22237	27666	13564	1326	24764	18410	21634	21721	18159
16489	7067	9746	20618	6334	13735	23970	6780	10956	11922	26721	19645	13232	19201	5718	3052	25575	14192	7565	25919
21700	25936	4682	4624	16551	3211	24006	22105	19236	11861	11102	5615	2987	1885	27899	3695	26259	18797	21600	24760
17070	11607	91	4509	20930	5418	28181	13889	5148	13543	9103	19934	1729	28357	25129	16971	19613	5978	11841	28061
7089	11151	25678	14257	2598	12212	24400	374	23885	49	20063	11270	713	12970	20705	2772	5088	7106	23960	931
17343	25134	5567	20763	19502	18428	14968	25861	3800	16031	14290	19034	19802	21956	26654	6248	26479	4190	14886	18019
26809	25265	4815	22236	18484	13334	10084	521	26760	5202	22202	21523	5514	21286	7312	24090	19654	9899	21271	12867
5387	1452	6759	18733	7092	10040	26368	16640	18013	15819	16382	27588	13793	12043	20120	18818	13823	933	27020	13991
12597	6002	2953	4924	20079	14897	4393	16127	7395	12457	10087	28067	27450	7585	8960	25130	26153	19843	25877	7427
25664	337	28035	20196	225	2646	23093	6783	9845	12612	447	6403	16839	11183	4275	21617	8912	14249	15113	10372
21456	20774	5876	20958	4601	5964	26578	24841	8999	10687	6466	22165	25673	25661	1448	27345	17813	13467	27696	2454
23798	3611	53	28134	12190	22995	23971	15962	11186	3164	22307	11295	1007	18720	2354	7050	25594	16708	11935	2802
10427	26334	19679	10193	27021	23173	24918	28245	28397	19868	26171	13177	1360	21725	26230	10432	14930	20829	23717	4951
23957	2042	7966	11148	26789	13567	215	25454	20793	8392	25328	10141	8069	11213	21822	28517	4085	25114	22526	16163
12150	28256	14771	22398	15804	21937	24138	1878	20939	2085	1594	21038	22736	24364	13706	15605	110	7025	25300	10958
19198	6829	2362	23192	27434	3958	5280	21973	10806	10158	20878	15123	16221	10793	5420	17888	14349	16289	4715	21060
6530	23361	13081	8560	12016	11618	21183	4078	22383	9512	20530	10339	1015	8656	13597	20640	24688	19711	8493	8226
22635	10080	22720	1629	24141	8016	3057	8255	20426	1462	15122	7247	18154	21359	21305	714	20714	6205	13531	17762
7739	8346	17447	7029	19937	14006	21107	20737	27181	767	11736	14171	28302	20124	12608	7039	400	20916	18487	9828
22152	28096	4194	13547	3697	18795	4154	5724	4714	618	19133	25840	10026	2129	21629	9632	15342	7288	26889	21033
10563	4704	20155	12223	28460	20935	7158	22957	17174	15966	3236	28218	830	11878	390	11796	11577	12448	4404	4468

Table 2: Showing the first 570 random numbers from the 514, 229 that was generated $(m = 514229, a = 518, x_0 = 211)$

211	392581	398518	101	119679	475901	202328	54850	369153	355182	418629	23166	496588	261314	503384	488725	266436	513912	316801
109298	236503	226495	52318	286242	201027	417417	129705	442295	404523	359413	172721	118084	118425	38809	158882	200476	350023	63867
51174	122052	80198	360816	175404	257728	245826	337420	276905	251711	25036	507861	488490	150899	48131	24236	486539	303306	172450
282453	486998	404244	237561	354968	317793	323305	459929	481128	286361	112923	300979	37152	2874	248866	212752	54992	272663	367483
269618	292754	107189	155867	293671	63494	347565	155195	337468	237046	386237	95735	218263	460274	355338	160530	203261	340688	91464
306065	463246	501399	5153	424023	493465	58520	171286	484793	403326	35685	224746	444083	333905	485331	363671	386482	95837	69284
159138	330714	39037	98109	68131	43057	488078	278760	179022	145894	486815	202674	174631	181846	457706	173764	162595	277582	407311
156844	71595	166235	426020	324286	191679	337965	413560	172176	495658	197960	82416	468783	92321	32139	19677	404883	317585	153208
511239	61722	233487	74119	341494	43525	228010	304816	225551	150573	211709	10481	113506	513210	192674	422335	438191	469979	170478
508096	89798	102451	340696	513345	434103	350739	26385	105435	348235	134485	286868	174002	500616	44706	222205	207949	218805	374445
422709	234754	104031	99981	56317	147281	159965	297476	107056	405580	242315	499672	142961	147672	17403	429123	243721	210610	98177
415937	244528	408242	367258	375382	185666	71001	338097	432505	285008	47294	172909	4822	388204	272861	138786	261373	79432	461244
507644	165170	121237	489143	69314	14165	268259	296386	347975	50421	329529	91016	440880	26133	443252	413317	148987	7456	322136
188573	196046	64828	375406	422851	138264	116332	287706	270900	406628	486223	351449	58164	166940	258402	178942	40916	262605	256252
491533	248715	156019	81746	489493	142921	95183	419527	455912	313643	405533	13516	303670	84448	152696	130736	111099	272934	67454
70739	277120	83889	177650	42477	498331	453039	310348	131305	484939	260662	316311	461215	34599	419491	357249	469863	481066	487829
132543	78269	259266	489938	405468	506729	185778	320816	137762	254650	294918	324276	307114	438496	291700	446771	158717	305352	208983
264817	433480	86019	272987	226992	228832	72181	86721	397114	266076	41511	336314	188291	365939	431503	24328	452995	304033	265104
390292	338796	334148	508520	337644	262306	365270	183555	13452	13996	419309	401250	345457	320130	343168	260408	162986	135020	24729
79259	144239	307720	128112	61732	118052	487817	463354	283159	50722	197424	98984	509263	245602	352019	163346	93192	5216	468126
432071	152597	502199	26475	94978	471914	202767	386658	121097	48317	448290	365041	512986	207273	308776	279672	450159	130743	287409
123163	368209	453437	344096	346849	192677	130590	253763	506537	345214	296941	369195	384584	407782	20749	371747	236625	360875	265681
34038	467532	391942	318494	201861	46260	281621	320839	129376	383389	60967	464051	207889	397186	463402	243300	185248	268123	323615
147898	493946	419730	426612	175511	308146	352871	98635	166998	103108	212937	233475	212641	50748	411522	43295	311870	45884	508145
505272	292215	415502	380775	410394	208638	235883	184259	114492	444357	256360	96235	103032	61785	277590	314963	80754	113378	448091
502564	184044	282314	291743	207515	86394	315121	313797	170521	316563	123398	483746	404989	122432	321729	140241	178023	107698	193859
128278	202427	197616	453777	18909	14169	222085	50482	396719	454812	155768	150905	493099	169609	45426	138549	168923	250832	144307
112463	468699	33517	53833	24511	140336	366963	438226	323071	75734	468100	5982	367698	438532	390363	290551	83184	345268	187821
147957	69994	392249	117128	355202	187759	336333	226079	226353	148808	273941	13302	202834	384587	116037	350550	408305	411361	101997
21605	260862	64527	507511	414883	69881	411092	378939	6642	462423	488463	205459	165296	209443	456602	62063	153871	194192	383088

5.

Conclusion

The uniqueness of Fibonacci sequence is been discussed with particular emphasis on its application to random number generation. The Lehmer's algorithm was employed using Fibonacci prime on a 32 bit machine. Two set of numerical experiments were carried out using a five and six digits fibonacci prime. Both experiments produce large sets of random numbers with full periods. Higher digits fibonacci primes could be studies for randomness and implementation. We suggest that further research be made to devise algorithms that help in finding the appropriate choice of full multiplier $a,$ modulus m (fibonacci prime) and a starting seed x_0 that will produce a full period.

References

Adam, J. A. (2006). Mathematics in Nature. Princeton University press, New Jersey

Bassein, S., (1996). A sampler of randomness. American Mathematical Monthly 103 (6): 483–489.

Conway, J. H. and Guy, R. K. (1996), "Fibonacci Numbers." In *The Book of Numbers.* New York: Springer-Verlag, pp. 111-113, 1996.

Fergusson, D. E. (1960), Fibonacci searching. *Communication ACM*, Vol. 3(12)

Hilton, P. and Pedersen, J.(1994) "A Note on a Geometrical Property of Fibonacci Numbers." *Fib. Quart.* **32**, 386-388, 1994.

Knuth, D. E. (1997), The Art of Computer Programming; *Fundamental Algorithms.* Vol. 1, 3rd ed. Reading, MA:Addison-Wesley.

Leemis L. M.and Park, S. K (2006). *Discrete-Event Simulation: A First Course*, pp. 42, Prentice Hall,

Livio, M. (2002), The Golden Ratio: The Story of Phi, the World's Most Astonishing Number. New York, Broadway Books,

Matthew, J. H. and Fink, K. D. (2004), Numerical Methods using MATLAB. 4th Ed. Prentice-Hall, New Jersey

Neave, H. R. (1973), On using the Box-Muller transformation with multiplicative congruential pseudorandom numbers generators. *Applied Statistics* 22, 92 – 97

von Neumann, J. (1951), Various techniques used in connection with random digits, *Appl. Math. Ser*., Notes by G.E. Forstyle, *Nat. Bur. Stand*., vol. 12, pp. 36–38, 1951.

Shorey, T. N. and Stewart, C. L. (1981) "On Divisors of Fermat, Fibonacci, Lucas and Lehmer Numbers, 2." *J. London Math. Soc.* **23**, 17-23