International Journal of Engineering, Science and Mathematics
Vol. 6Issue 8, December 2017,(Special Issue)
ISSN: 2320-0294 Impact Factor: 6.765
Journal Homepage: http://www.ijesm.co.in, Email: ijesmj@gmail.com
Double-Blind Peer Reviewed Refereed Open Access International Journal - Included in the International Serial Directories Indexed & Listed at: Ulrich's Periodicals Directory ©, U.S.A., Open J-Gage as well as in Cabell's Directories of Publishing Opportunities, U.S.A

Note on Fibonacci Pseudoprimes

Prof. Dr.K. Raja RamaGandhi *
D. NarasimhaMurty**

Abstract

We define various types of Fibonacci and Lucas peseudoprimes and prove some theorems on these pseudoprimes. In particular, we will discuss the existence of Fibonacci pseudoprimes by setting some parameters.

Keywords:

Fibonacci number;
Lucas number;

Author correspondence:

Prof. Dr.K. Raja RamaGandhi,
Resourceperson inMath forOxfordUniversityPress and Professor in Mathematics.

1. Introduction

We know that every non-absolute compositeness test series rise to a class of Pseudoprimes. The same, we can see in the case of Fibonacci number [1], which are recursively defined by

$f_0 = 0,\ f_1 = 1$ and $f_n = f_{n-1} + f_{n-2} \forall n \geq 2$

i.e $0,1,1,2,3,5,8,13,...$

the sequence corresponding to $(P,Q) = (1,-1)$ $U_0(1,-1) = 0$ and $U_1(1,-1) = -1$ was first consider by Fibonacci, and it begins as

$0,1,1,2,3,4,5,8,13,...323,...$

Since Fibonacci number grow quite large, in order to evaluate f_n efficiently we can use matrix identity.

$$\begin{bmatrix} f_{N+1} \\ f_N \end{bmatrix} = F^n \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \text{ where } F = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$$

Justification: The above identity can be proved by induction.

For instance, the first FibonacciPseudoprime is 323

i.e. $323 = 17X19,$

* Doctorate Program, Linguistics Program Studies, Udayana University Denpasar, Bali-Indonesia (9 pt)
** STIMIK STIKOM-Bali, Renon, Depasar, Bali-Indonesia

Now, we will show that $323 | f_{324}$ by successive squaring algorithm,

$$F^2 = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}$$

$$F^4 = \begin{bmatrix} 2 & 1 \\ 0 & 1 \end{bmatrix}^2 = \begin{bmatrix} 5 & 3 \\ 2 & 1 \end{bmatrix}$$

$$F^8 = \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix} = \begin{bmatrix} 34 & 21 \\ 21 & 13 \end{bmatrix}$$

$$F^{16} = \begin{bmatrix} 34 & 21 \\ 21 & 13 \end{bmatrix}^2 = \begin{bmatrix} 305 & 18 \\ 18 & 287 \end{bmatrix}$$

$$F^{32} = \begin{bmatrix} 305 & 18 \\ 18 & 287 \end{bmatrix}^2 = \begin{bmatrix} 2 & 320 \\ 320 & 5 \end{bmatrix}$$

$$F^{64} = \begin{bmatrix} 2 & 320 \\ 320 & 5 \end{bmatrix}^2 = \begin{bmatrix} 13 & 320 \\ 320 & 34 \end{bmatrix}$$

$$F^{128} = \left(F^{64}\right)^2 = \begin{bmatrix} 287 & 305 \\ 305 & 305 \end{bmatrix}$$

$$F^{256} = \left(F^{128}\right)^2 = \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix}$$

$$F^{324} = F^{256} \text{ X } F^{64} \text{ X } F^4$$

$$= \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix} \begin{bmatrix} 13 & 320 \\ 320 & 34 \end{bmatrix} \begin{bmatrix} 5 & 3 \\ 3 & 2 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = I$$

By the above results we say the $323 | f_{324}$

Note: one can try the same, using larger Fibonacci Pseudoprimes in the case of

$377, 1891, 3827$ and 4181

2. Finding with Justifications

As we shown/discussed in earlier introduction, the following theorems are defined:

Theorem 2.1: $P | f_{p-1}$ if $P = \pm 1 (\mathrm{mod} 10)$ and $P | f_{p+1}$ if $P = \pm 3 (\mathrm{mod} 10)$

Proof: Leaving for readers.

Let us discuss the following important theorems

Theorem 2.2: with parameters $P=1$ and $Q=-1$, there do not exist even Fibonacci Pseudoprime.

Before solving this theorem, we define the following.

Observation#1: $A=P^2-P-2Q$ admits an odd prime divisor $p=4k$ $(k\in z^+)$ and $Q=\{-1,1\}$

Justification: $A=(4k)^2-4k-2Q$

$A=2(\text{mod}4)$, if $A=\pm 2$ then A admits an odd prime divisor.

Observation#2: If $p=4k+1$ $(k\in z)$ and $Q=\{-1,1\}$ then the value $A=P^2-P-2Q$ admits an odd prime divisor $P\neq 3$, unless $(P,Q)=(1,-1)$, $(P,Q)=(1,1)$ or $(P,Q)=(5,1)$.

Justification: By observation #1, we have $P=1(\text{mod}4)$ and $A=2(\text{mod}4)$ if $Q=-1$

$\Rightarrow P^2-P+2=\pm 2$ iff $P=1$

Now, $A=\pm 1(\text{mod}3)$

Here A admits an odd prime divisor $P\neq 3$ and $P\neq 1$

Or for $Q=1$, we have $P^2-P-2=\pm 2$ Iff $P=1$

Here $A=0(\text{mod}3)$ when $P=2(\text{mod}3)$

Here A admits an odd prime divisor $P\neq 3$.

Observation#3: let $\{a_n\}$ is defined by recurrence relation $a_{k+1}=a_k{}^2-2,\ k\geq 1$

If $a_1=2l(l\in z)$, then $a_k=2(\text{mod}2^k),\ k\geq 1$

If $a_1=2l+1$, then $a_k=-1(\text{mod}2^k),\ k\geq 1$.

3. Justification

Let us consider that $a_k=\alpha(\text{mod}2^k)$

Here $k\geq 1$ and $\alpha=-1$ or 2

Clearly, $\alpha^2-2=\alpha$

$$a_k-\alpha=2^k t$$

Or $$a_k=\alpha+2^k t\ (t\in z)$$

And $a_{k+1}=a_k{}^2-2$

$$=\left(\alpha+2^k t\right)^2-2$$

$$=\alpha^2+\left(2^k t\right)^2+2\alpha 2^k t-2$$

$$=\left(\alpha^2-2\right)+2^{k+1}\left(\alpha t+t^2 2^{k-1}\right)$$

$$\equiv \alpha^2-2=\alpha\left(\text{mod}2^{k+1}\right)$$

Now, we can define some lemmas based on above observations:

Lemma#1: For $P=1=Q$, no every Fibonacci Pseudo Prime exists.

Proof: Let us consider sequence $\{V_n\}$ with recurrence relation $V_0=2$, $V_1=1$

$$V_n=V_{n-1}-V_{n-2}$$

$$V_1=1$$

$$V_2=V_1-V_0=1-2=-1$$

$$V_3=V_2-V_1=-1-1=-2$$

$$V_4=V_3-V_2=-2+1=-1$$

$$V_5=V_4-V_3=-1+2=1$$

$$V_6=V_5-V_4=1-(-1)=2$$

$$V_7=V_6-V_5=2-1=1$$

$$V_8=V_7-V_6=1-2=-1$$

$\{V_n\}$ is periodic with period 6.

i.e. $V_{6k}=2$, $k\geq 0$

and $V_{6k\pm 2}=-1$, $k\geq 0$

$\therefore$ Every Fibonacci Pseudo Prime does not exist. [2],[3] and [4]

Lemma#2: For $n=2^k$, $k\geq 2$, $Q=\{-1,1\}$ iff $P=2(\mathrm{mod}\,2^k)$ or $P=-1(\mathrm{mod}\,2^k)$.

Proof: For $n\geq 0, V_{2n}=V_n^{\,2}-2Q^n$ from observation #3,

we have $a_{k+1}=a_k^{\,2}-2$, $k\geq 1\rightarrow$ (1)

$V_{2n}=V_n^{\,2}-2Q$ deduce that $V_{2^{k+1}}=V_{2^k}^{\,2}-2(\pm 1)^{2^k}$

$$=V_{2^k}^{\,2}-2\ ,\ k\geq 1$$

Thus $a_k=V_{2^k}$ satisfies observation #3 or Equation (1)

Also $$a_1=V_2=P^2-2Q$$

$$\equiv P^2\equiv P(\mathrm{mod}\,2)$$

By observation #3; $V_{2^k}=2(\mathrm{mod}\,2^k)$ if $k\geq 1$ and $P=2l$

Then $V_{2^k}\equiv -1(\mathrm{mod}\,2^k)$

Lemma#3: If $P\equiv 0(\mathrm{mod}\,4)$ or $P\equiv 1(\mathrm{mod}\,4)$ with $(P,Q)\neq(5,1)$ and $P\neq 1$ then there exists an odd prime number P such that $n=2P$ is an even number.

Proof: We know that;

(a) If $P=2l$ then $V_n\equiv 0(\mathrm{mod}\,2)$; $n\geq 0$

(b) If $P = 2l+1$ then $V_n \equiv 0(\mathrm{mod}\,2)$ iff $n = 0(\mathrm{mod}\,3)$

(c) If P is prime, then $V_{np} \equiv V_n(\mathrm{mod}\,P)$ for $n \geq 0$.

Let us assume that $P \equiv 0(\mathrm{mod}\,4)$ or $P \equiv 1(\mathrm{mod}\,4)$ and the P is odd prime.

Here $V_{2p} \equiv P(\mathrm{mod}\,2P)$ is similar to $V_{2p} \equiv P(\mathrm{mod}\,2) \rightarrow (2)$

and $V_{2p} \equiv P(\mathrm{mod}\,P) \rightarrow (3)$

by (a) and (b), the relation (2) is true

by (c) relation (3) holds.

Proof: The cited above observations/Lemma's concludes the theorem.

APPENDIX

I. Conditional Identities

We can define the following identities:

I. $U_n = PU_{n-1} - QU_{n-2}(n \geq 2), U = 0, U_1 = 1$

$V_n = PV_{n-1} - QV_{n-2}(n \geq 2), V_0 = 2, V_1 = p$

II. $U_{2n} = U_n V_n$

$V_{2n} = V_n^{\,2} - 2Q^n$

III. $U_{m+n} = U_m V_n - Q^n U_{m-n}$

$V_{m+n} = V_m V_n - Q^n V_{m-n}$ (for $m \geq b$)

IV. $U_{m+n} = U_m U_{n+1} - QU_{m-1}U_n$

$V_{m+n} = (V_m V_n + DU_m V_n)/2$

V. $DU_n = 2V_{n+1} - PV_n$

$V_n = 2U_{n+1} - PU_n$

VI. $U_n^{\,2} = U_{n-1}U_{n+1} + Q^{n-1}$

$V_n^{\,2} = DU_n^{\,2} + 4Q^n$

VII. $U_m V_n - U_n V_m = 2Q^n U_{m-n}\ (m \geq n)$

$U_m V_n + U_n V_m = 2U_{m+n}$

VIII. $2^{n-1}U_n = \binom{n}{c_1} p^{n-1}D^0 + \binom{n}{c_3} p^{n-3}D^1 + \binom{n}{c_5} p^{n-5}D^2 + \ldots$

$2^{n-1}V_n = \binom{n}{c_0} p^n D^0 + \binom{n}{c_2} p^{n-2}D^1 + \binom{n}{c_4} p^{n-4}D^2 + \ldots$

IX. $U_n \equiv V_{n-1}(\mathrm{mod}\,Q)$

$V_n \equiv P^n (\mathrm{mod} Q)$

X. $V_p \equiv P(\mathrm{mod} P)$

XI. $U_m = V_{m-1} + QV_{m-3} + Q^2 V_{m-5} + \ldots +$ (last sum and); where

Last sum and = $\begin{cases} Q^{\frac{m-2}{2}} \; if \; m=Even \\ Q^{\frac{m-1}{2}} \; if \; m=Odd \end{cases}$

II. Fibonacci and Lucas numbers for $P = 1, Q = -1$

Fibonacci number	**Lucas number**
U(0)=1,U(1)=1	V(0)=2,V(1)=1
U(2)=1	V(2)=3
U(3)=2	V(3)=4
U(4)=3	V(4)=7
U(5)=5	V(5)=11
U(6)=8	V(6)=18
U(7)=13	V(7)=19
U(8)=21	V(8)=47
U(9)=34	V(9)=76
U(10)=55	V(10)=123
U(11)=89	V(11)=199
U(12)=144	V(12)=322
U(13)=233	V(13)=521
U(14)=377	V(14)=843
U(15)=610	V(15)=1364
U(16)=987	V(16)=2207
U(17)=1597	V(17)=3571
U(18)=2584	V(18)=5778
U(19)=4181	V(19)=9349
U(20)=6765	V(20)=15127
U(21)=10946	V(21)=24476
U(22)=17711	V(22)=39603

References

[1] Alfred S. Posamentier, Ingmar Lehmann. "*The Fabulous Fibonacci Numbers*", Prometheus Books, 2007.

[2] Paulo Ribenboim. "*The Little Book of Bigger Primes*", Springer publication, Canada, 1991

[3] Andreas Philippou, Alwyn F. Horadam, G.E. Bergum. "*Applications of Fibonacci Numbers*", Springer Science + Business Media LLC, CIP, 1986.

[4] Abhijit Das ."*Computational Number Theory*", CRC Press, 2013.