ON A CONGRUENCIAL PROPERTY OF FIBONACCI NUMBERS — NUMERICAL EXPERIMENTS —

MASATAKA YORINAGA

1. Introduction. Let (U_n) be the sequence of Fibonacci numbes, that is, a sequence of integers defined by

$$U_0=0,\ U_1=1,\ U_n=U_{n-1}+U_{n-2}\quad (n=2, 3, \cdots),$$

and let $\left(\frac{n}{5}\right)$ be Legendre's symbol, so that

$$\left(\frac{n}{5}\right)=\begin{cases} 1 & \text{if } n\equiv 1,\ 4 \pmod 5 \\ -1 & \text{if } n\equiv 2,\ 3 \pmod 5. \end{cases}$$

Then, the following proposition is well known in standard textbooks of the theory of numbers (cf. e. g. [2]).

Proposition. *If n is a prime number $\neq 5$, then we have*

$$U_n\equiv\left(\frac{n}{5}\right) \pmod n.$$

Recently, Prof. S. Uchiyama proposed the author to carry out a numerical experiment examining whether the converse of the above proposition is true or untrue. Namely, the problem is this : if $U_n\equiv\left(\frac{n}{5}\right) \pmod n$, then is n necessarily a prime ?

We have solved negatively this problem*) by means of a computer calculation and the present note is a report of the result obtained in our experiments.

2. Principle. Let $N=a_0a_1a_2\cdots a_t$ be the binary representation of an integer $N>0$ where $a_0=1$, $a_i=0$ or 1 $(i=1, 2, \cdots, t)$ are binary digits of N and $t+1$ is the number of binary digits.

The first point with which we are confronted is how to compute the value of $U_n \pmod n$ for fairly large n. In this situation, it is not much effective to compute $U_n \pmod n$ by its definition. Our fundamental for-

*) The problem was actually posed by Prof. D. Sato in University of Regina, Canada, in a private communication. One may easily verify that if $n\equiv 21$ or $35 \pmod{56}$, then $U_n\not\equiv\pm 1 \pmod n$.

mulas are as follows:

$$U_{2n-1}=U_{n-1}^2+U_n^2,$$
$$U_{2n}=(2U_{n-1}+U_n)U_n,$$
$$U_{2n+1}=(U_{n-1}+U_n)^2+U_n^2.$$

These formulas are easily derived from the definition and basic relations of Fibonacci numbers [1, 3].

Now, for the moment, to avoid the trouble of double suffix, we denote $U_k \pmod N$ by $U(k)$. We define the sequence of integers s_i as follows:

$$s_0=a_0=1$$
$$s_i=2s_{i-1}+a_i \quad (i=1,\ 2,\ \cdots,\ t).$$

Obviously, $N=s_t$. Put $U(0)=0$, $U(1)=1$. When values of $U(s_{i-1}-1)$ and $U(s_{i-1})$ are known, then $U(s_i-1)$ and $U(s_i)$ can be obtained by use of the fundamental formulas. More precisely, if $a_i=0$, then $U(s_i-1)$ and $U(s_i)$ are computed with the modulus N by use of the upper two formulas and if $a_i=1$, then they are computed by the lower two of them. Hence, we can obtain $U(s_t)\equiv U_N \pmod N$ for relatively small number of steps.

The second point is the multiplication of two numbers with the modulus N.

Let A and B be given two integers and let $B=b_0b_1\cdots b_t$ be the binary representation of B. We adopt the following scheme:

$$C_0=b_0A,$$
$$C_i\equiv 2C_{i-1}+b_iA \quad (i=1,\ 2,\ \cdots,\ t) \pmod N.$$

In this manner, we can obtain the product $C_t\equiv AB \pmod N$ by taking no care of overflow in an accumulator of a computer.

3. Procedure. In the following, we state schematically the actua lprocedure.

Step 1 : Read a starting value N. Reset $N\equiv 1 \pmod 5$.
Step 2 : Store $a_1,\ a_2,\ \cdots,\ a_t$ and t to the memory.
Step 3 : Set P(1)=0, Q(1)=1 and $k=1$.
Step 4 : Take up a_k.
If $a_k=1$, then go to the Step 6.
Step 5 : $P(k+1)\equiv P(k)^2+Q(k)^2 \pmod N$,
$Q(k+1)\equiv(2P(k)+Q(k))Q(k) \pmod N$,
then go to the Step 7.
Step 6 : $P(k+1)\equiv(2P(k)+Q(k))Q(k) \pmod N$,
$Q(k+1)\equiv(P(k)+Q(k))^2+Q(k)^2 \pmod N$.

Step 7 : Replace $k+1$ to k.
If $k<t$, then go to the Step 4.

Step 8 : Compare $Q(t)$ with $\left(\frac{N}{5}\right)$.

If they are not equal, then go to the Step 10.

Step 9 : Test the primality of N.
Print the result.

Step 10 : Replace $N+1$ to N.
If $N \not\equiv 0 \pmod 5$, then go to the Step 2.

Step 11 : Replace $N+1$ to N, then go to the Step 2.

4. Observations. In this experiment, we have computed the value of U_N up to $N \leqq 707000$ and we have found many composite numbers N satisfying $U_N \equiv \left(\frac{N}{5}\right) \pmod N$.

In the following table, we list these numbers with their factorization. At a glance, a definite regularity is not found in the sequence of such numbers. Nevertheless, we have observed somewhat plausible characters.

(i) Distribution of values of N in the modulus 5 is as follows :

$N \pmod N$	1	2	3	4	total
Number of N	41	14	21	33	109

Appearence of 1 is slightly more often than others. May one regard this phenomenon as a fluctuation ?

(ii) It seems that distribution of prime factors does not spread over all primes. Within the bound 200, the prime factors which do not appear are the following 6 primes : 67, 97, 127, 157, 179, 191. Is this phenomenon a proper character ?

(iii) In the early stage of our experiment, it was anticipated that the numbers in question did not satisfy that $2^{N-1} \equiv 1 \pmod N$. However, we found the number $N=252601$ which satisfied the both conditions, namely, $U_{252601} \equiv 1$ and $2^{252600} \equiv 1 \pmod{252601}$.

(iv) If n is an odd integer, then there holds the relation $U_n^2 - 1 = U_{n-1} U_{n+1}$. From this relation, one can derive the well known

Proposition. *If n is a prime number $\neq 5$, then*

$$U_{n-1} \equiv 0 \pmod n \text{ if } \left(\frac{n}{5}\right) = 1,$$

$$U_{n+1}\equiv 0 \pmod{n} \text{ if } \left(\frac{n}{5}\right) = -1.$$

We have examined that in what extend the above proposition is satisfied. As a result, we have recognized that there occurred all of the possible cases of combination except for one case. In the following, we have used the well known facts that:

(a) If $n=ab$, then U_n is divisible by U_a and U_b.

(b) U_{n-1} and U_{n+1} are coprime for any n.

Example 1. $N=4181=37\cdot 113$.

37 and 113 are the primitive factors of U_{19}.

$4180=2^2\cdot 5\cdot 11\cdot 19$ is divisible by 19.

Hence, U_{4180} is divisible by $37\cdot 113$. This is the case where $U_{N-1}\equiv 0 \pmod{N}$ and $\left(\frac{N}{5}\right)=1$.

Example 2. $N=6479=11\cdot 19\cdot 31$.

11 is the primitive factor of U_{10}.

19 〃 U_{18}.

31 〃 U_{30}.

$6480=2^4\cdot 3^4\cdot 5$ is divisible by $LCM(10, 18, 30)$.

Hence, U_{6480} is divisible by $11\cdot 19\cdot 31$. This is the case where $U_{N+1}\equiv 0 \pmod{N}$ and $\left(\frac{N}{5}\right)=1$.

Example 3. $N=5777=53\cdot 109$.

53 and 109 are the primitive factors of U_{27}.

$5778=2\cdot 3^3\cdot 107$ is divisible by 27.

Hence, U_{5778} is divisible by $53\cdot 109$. This is the case where $U_{N+1}\equiv 0 \pmod{N}$ and $\left(\frac{N}{5}\right)=-1$.

Example 4. $N=27071=11\cdot 23\cdot 107$.

11 is the primitive factor of U_{10}.

23 〃 U_{24}.

107 〃 U_{36}.

$27070=2\cdot 5\cdot 2707$ is divisible by 10 and $27072=2^6\cdot 3^2\cdot 47$ is divisible by $LCM(24, 36)$.

Hence, U_{27070} is divisible by 11 and U_{27072} is divisible by $23\cdot 107$. This is the case where the prime factors of N are partitioned into two classes of factors of U_{N-1} and U_{N+1} and $\left(\frac{N}{5}\right)=1$.

Example 5. $N=300847=37\cdot 47\cdot 173$.

37 is the primitive factor of U_{19}.
47 〃 U_{16}.
173 〃 U_{87}.

$300846=2\cdot3\cdot7\cdot13\cdot19\cdot29$ is divisible by $LCM(19, 87)$ and $300848=2^4\cdot18803$ is divisible by 16.

Hence, U_{300846} is divisible by $37\cdot113$ and U_{300848} is divisible by 47. This is the case where the prime factors of N are partitioned into two and $\left(\frac{N}{5}\right)=-1$.

The case where $U_{n-1}\equiv0 \pmod N$ and $\left(\frac{N}{5}\right)=-1$ did not happen in our experiments.

The program was written by an assembly language and the computation was done on a computer HITAC 10 in the Department of Mathematics, Okayama University.

REFFERENCES

[1] L. E. DICKSON: History of the the theory of numbers, Volume I, Chelsea Publ. Co., New York, 1952.
[2] G. H. HARDY and E. M. WRIGHT: An introduction to the theory of numbers, 3rd ed. Clarendon Press, Oxford, 1954.
[3] N. N. VOROB'EB: Fibonacci numbers, (English translation), Pergamon Press, Oxford, 1961.

DEPARTMENT OF MATHEMATICS
OKAYAMA UNIVERSITY

(*Received November 22, 1976*)

Table

$4181 = 37 \cdot 113$
$5474 = 2 \cdot 7 \cdot 17 \cdot 23$
$5777 = 53 \cdot 109$
$6479 = 11 \cdot 19 \cdot 31$
$6721 = 11 \cdot 13 \cdot 47$
$10877 = 73 \cdot 149$
$12958 = 2 \cdot 11 \cdot 19 \cdot 31$
$13201 = 43 \cdot 307$
$15251 = 101 \cdot 151$
$17302 = 2 \cdot 41 \cdot 211$
$27071 = 11 \cdot 23 \cdot 107$
$34561 = 17 \cdot 19 \cdot 107$
$40948 = 2^2 \cdot 29 \cdot 353$
$41998 = 2 \cdot 11 \cdot 23 \cdot 83$
$44099 = 11 \cdot 19 \cdot 211$
$47519 = 19 \cdot 41 \cdot 61$
$51841 = 47 \cdot 1103$
$54839 = 29 \cdot 31 \cdot 61$
$64079 = 139 \cdot 461$
$64681 = 71 \cdot 911$
$65471 = 7 \cdot 47 \cdot 199$
$67861 = 79 \cdot 859$
$68251 = 131 \cdot 521$
$72831 = 3 \cdot 11 \cdot 2207$
$75077 = 193 \cdot 389$
$78089 = 11 \cdot 31 \cdot 229$
$88198 = 2 \cdot 11 \cdot 19 \cdot 211$
$90061 = 113 \cdot 797$
$95038 = 2 \cdot 19 \cdot 41 \cdot 61$
$96049 = 139 \cdot 691$
$97921 = 181 \cdot 541$
$100127 = 223 \cdot 449$
$109871 = 17 \cdot 23 \cdot 281$
$113573 = 137 \cdot 829$
$118441 = 83 \cdot 1427$
$130942 = 2 \cdot 7 \cdot 47 \cdot 199$
$133742 = 2 \cdot 7 \cdot 41 \cdot 233$
$139359 = 3 \cdot 11 \cdot 41 \cdot 103$
$146611 = 271 \cdot 541$
$156178 = 2 \cdot 11 \cdot 31 \cdot 229$
$157079 = 13 \cdot 43 \cdot 281$
$160378 = 2 \cdot 17 \cdot 53 \cdot 89$
$161027 = 283 \cdot 569$
$162133 = 73 \cdot 2221$
$163081 = 17 \cdot 53 \cdot 181$
$163438 = 2 \cdot 11 \cdot 17 \cdot 19 \cdot 23$
$168299 = 31 \cdot 61 \cdot 89$
$186961 = 31 \cdot 37 \cdot 163$
$196559 = 11 \cdot 107 \cdot 167$
$197209 = 199 \cdot 991$
$203942 = 2 \cdot 107 \cdot 953$
$219742 = 2 \cdot 17 \cdot 23 \cdot 281$
$219781 = 271 \cdot 811$
$231703 = 263 \cdot 881$
$233519 = 11 \cdot 13 \cdot 23 \cdot 71$
$252404 = 2^2 \cdot 89 \cdot 709$
$252601 = 41 \cdot 61 \cdot 101$
$254321 = 263 \cdot 967$
$257761 = 7 \cdot 23 \cdot 1601$
$268801 = 13 \cdot 23 \cdot 29 \cdot 31$
$272611 = 131 \cdot 2081$
$283361 = 13 \cdot 71 \cdot 307$
$300847 = 37 \cdot 47 \cdot 173$
$302101 = 317 \cdot 953$
$303101 = 101 \cdot 3001$
$314158 = 2 \cdot 13 \cdot 43 \cdot 281$
$327359 = 23 \cdot 43 \cdot 331$
$330929 = 149 \cdot 2221$
$336598 = 2 \cdot 31 \cdot 61 \cdot 89$
$389666 = 2 \cdot 23 \cdot 43 \cdot 197$
$390598 = 2 \cdot 13 \cdot 83 \cdot 181$
$393118 = 2 \cdot 11 \cdot 107 \cdot 167$
$399001 = 31 \cdot 61 \cdot 211$
$417601 = 19 \cdot 31 \cdot 709$
$430127 = 463 \cdot 929$
$433621 = 199 \cdot 2179$
$438751 = 541 \cdot 811$
$451979 = 11 \cdot 17 \cdot 2417$
$467038 = 2 \cdot 11 \cdot 13 \cdot 23 \cdot 71$
$480478 = 2 \cdot 79 \cdot 3041$
$486359 = 29 \cdot 31 \cdot 541$
$489601 = 7 \cdot 23 \cdot 3041$
$510719 = 11 \cdot 29 \cdot 1601$
$512461 = 31 \cdot 61 \cdot 271$
$520801 = 241 \cdot 2161$
$530611 = 461 \cdot 1151$
$534508 = 2^2 \cdot 13 \cdot 19 \cdot 541$
$544159 = 7 \cdot 11 \cdot 37 \cdot 191$
$545279 = 7 \cdot 61 \cdot 1277$
$553679 = 7 \cdot 19 \cdot 23 \cdot 181$
$553839 = 3 \cdot 11 \cdot 13 \cdot 1291$
$556421 = 431 \cdot 1291$
$568342 = 2 \cdot 29 \cdot 41 \cdot 239$
$575599 = 41 \cdot 101 \cdot 139$
$618639 = 3 \cdot 7 \cdot 89 \cdot 331$
$620279 = 11 \cdot 17 \cdot 31 \cdot 107$
$635627 = 563 \cdot 1129$
$636641 = 461 \cdot 1381$
$638189 = 619 \cdot 1031$
$640798 = 2 \cdot 17 \cdot 47 \cdot 401$
$641199 = 3 \cdot 13 \cdot 41 \cdot 401$
$654626 = 2 \cdot 7 \cdot 19 \cdot 23 \cdot 107$
$654718 = 2 \cdot 23 \cdot 43 \cdot 331$
$655201 = 23 \cdot 61 \cdot 467$
$670879 = 11 \cdot 71 \cdot 859$
$680578 = 2 \cdot 17 \cdot 37 \cdot 541$
$689359 = 11 \cdot 29 \cdot 2161$
$697034 = 2 \cdot 13 \cdot 17 \cdot 19 \cdot 83$
$701569 = 11 \cdot 23 \cdot 47 \cdot 59$