

$$K = 7, D = 3628800$$

1103970	1062720	1073250	1067520	1073250	1062720	1103970		
4195470	5629440	5503950	5560320	5508750	5598720	5258190		
-3653910	-613440	1115370	829440	1046250	699840	1944810		
3693990	2350080	4800870	6850560	6243750	7050240	4393830		
-2656410	-1849920	-2456730	-407040	2043750	699840	4393830		
1244970	898560	1115370	829440	2558250	5598720	1944810		
-340530	-250560	-302130	-245760	-371250	1062720	5258190		
41250	30720	36450	30720	41250	0	1103970		
-33953	-26656	-29889	-27392	-30625	-23328	-57281		

$$\begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_k \\ H \end{bmatrix} = C_k \begin{bmatrix} a_1 \\ a_2 \\ \vdots \\ a_k \end{bmatrix}$$

$$K = 8, D = 7257600$$

2140034	2072128	2086722	2080256	2085250	2078784	2093378	2025472	
8934188	11685376	11486124	11558912	11507500	11570688	11432876	12058624	
-9209188	-2719616	556956	124928	377500	93312	681884	-1900544	
11190716	7685632	12949308	16769024	15917500	16713216	15203132	21495808	
-10066240	-7431680	-9097920	-4648960	-200000	-1866240	768320	-9297920	
6292676	4782592	5578308	4726784	8546500	13810176	10305092	21495808	
-2582428	-1993856	-2278044	-2025472	-2457500	819072	7308644	-1900544	
625748	487936	551124	499712	572500	373248	3124436	12058624	
-67906	-53312	-59778	-54784	-61250	-46656	-114562	2025472	
57281	46656	50625	48128	50625	46656	57281	0	

The Boeing Company
 Renton, Washington
 Now at
 University of Alberta
 Calgary, Alta, Canada

1. G. DAHLQUIST, "Convergence and stability in the numerical integration of ordinary differential equations," *Math. Scand.*, v. 4, 1956, p. 33-53.
2. T. E. HULL, & A. C. R. NEWBERY, "Integration procedures which minimize propagated errors," *J. Soc. Indust. Appl. Math.*, v. 9, 1961, p. 31-47.
3. ———, "Corrector formulas for multi-step integration methods," *J. Soc. Indust. Appl. Math.*, v. 10, 1962, p. 351-369.
4. H. A. ANTOSIEWICZ & W. GAUTSCHI, "Numerical methods in ordinary differential equations," *A Survey of Numerical Analysis*, Editor, J. Todd, McGraw-Hill Book Co., New York, 1962, p. 314-346.

On the Non-Existence of Fibonacci Squares

By M. Wunderlich

The Fibonacci sequence, F_n , is defined as follows:

$$(1) \quad F_1 = 1; \quad F_2 = 1; \quad F_n = F_{n-2} + F_{n-1} \quad \text{for } n > 2.$$

A. P. Rollet [1] has posed the following problem. There are only three known Fibonacci numbers which are squares; $F_1 = 1$, $F_2 = 1$, and $F_{12} = 144$. Are there any others? The purpose of this note is to announce that except for the known cases, F_n cannot be a square for $n \leq 1,000,000$, and to describe the computational method used to arrive at this result. The referee has kindly pointed out that the method used is somewhat analogous to familiar "exclusion" methods such as those described in [2].

Let p be an arbitrary fixed prime number. With respect to this prime, denote by

Received November 20, 1962, revised April 10, 1963.

\bar{F}_n the least positive residue of F_n modulo p . We will then refer to the sequence $\bar{F}_1, \bar{F}_2, \bar{F}_3, \dots$ as the "reduced Fibonacci sequence." The mathematical basis for the method depends on the following elementary property of this sequence.

THEOREM. *The reduced Fibonacci sequence is purely periodic of period less than p^2 , that is, there exists an $N \leq p^2$ such that*

$$n \equiv m(N) \text{ implies } \bar{F}_n = \bar{F}_m.$$

Proof. Consider the p^2 pairs of numbers

$$(2) \quad (\bar{F}_1, \bar{F}_2), \quad (\bar{F}_2, \bar{F}_3), \quad \dots \quad (\bar{F}_{p^2}, \bar{F}_{p^2+1})$$

If each of the pairs is distinct from each other, then one of them must assume the value $(0, 1)$ since there are only p^2 pairs of numbers modulo p . If $(\bar{F}_t, \bar{F}_{t+1}) = (0, 1)$, then it is clear that $(\bar{F}_{t+1}, \bar{F}_{t+2}) = (1, 1) = (F_1, F_2)$, and the reduced sequence will be periodic with period t . If, on the other hand, two of the pairs in (2) are equal, say

$$\begin{aligned} (\bar{F}_r, \bar{F}_{r+1}) &= (\bar{F}_m, \bar{F}_{m+1}), & \text{where } r < m, \text{ then we have} \\ (\bar{F}_{r-1}, \bar{F}_r) &= (\bar{F}_{m-1}, \bar{F}_m), & \text{and hence} \\ (\bar{F}_{r-2}, \bar{F}_{r-1}) &= (\bar{F}_{m-2}, \bar{F}_{m-1}), & \text{and eventually} \\ (\bar{F}_1, \bar{F}_2) &= (\bar{F}_{r-m}, \bar{F}_{r-m+1}) = (1, 1). \end{aligned}$$

Hence the reduced sequence is periodic of period $r - m - 1$. Q. E. D.

Now let

$$(3) \quad \bar{F}_1, \bar{F}_2, \dots, \bar{F}_M$$

be the first cycle of the sequence of reduced Fibonacci numbers, and let

$$\bar{F}_{t_1}, \bar{F}_{t_2}, \dots, \bar{F}_{t_k}$$

be the elements of (3) which are equal to quadratic non-residues mod p . Then for $1 \leq h \leq k$, and $n \equiv t_h(M)$, we have from the theorem that $\bar{F}_n = \bar{F}_{t_h}$. Since \bar{F}_n is a quadratic non-residue mod p , F_n cannot be a square.

On the basis of probability considerations alone, it may be expected that approximately one half of the numbers in (3) are quadratic non-residues modulo p . Hence when applying this argument to a finite set of Fibonacci numbers it may be expected to roughly halve the number of them which could be squares. Hence if one wishes to prove that the first 1,000,000 Fibonacci numbers contains only the three known squares, this argument would have to be repeated approximately $\log 1,000,000 / \log 2$ times, or approximately 20 times. Of course since this estimate is based on probability arguments alone, it is conceivable that it may take more repetitions to verify the result.

In order to program this sieve on the 709 I.B.M. computer, it was necessary to reserve one million storage locations in the machine, one for each of the first million Fibonacci numbers. Since for each of these numbers we had to determine whether it is not a square or could be a square, it was possible to use a single binary unit, a bit, for each of these locations. Therefore, we reserved one million consecu-

tive bits to represent the first one million Fibonacci numbers and we adopted the following convention: If a one occupied the n th bit, this meant that F_n could be a square. If a zero occupied the n th bit, F_n could not be a square. These bits, which we shall call Fibonacci bits, were originally all set to contain ones.

In order to describe the program it is best to consider a special case. Let p be the prime 7. The first cycle of the sequence of reduced Fibonacci numbers are the 16 numbers

$$(4) \quad 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0.$$

The quadratic non-residues of 7 are the numbers 3, 5, and 6. If we rewrite (4) replacing the quadratic residues by ones and the quadratic non-residues by zeros and omitting the commas, we get

$$(5) \quad 1110010100011011.$$

In the program this expression was actually constructed as a binary number which was then used as a mask on the Fibonacci bits. Since there are 16 bits in (5) the masking was executed as follows: If a zero occurred in the n th bit of (5), zeros replaced all the m th Fibonacci bits where $m \equiv n(16)$. If a one was in the n th bit of (5), the m th Fibonacci bits were unchanged. The 709 I.B.M. computer contains a single instruction which will perform such a logical operation on a single word of 36 bits. Therefore our mask could be performed with this instruction together with a series of shifting and storing instructions.

The entire program consisted of repeating this process with successive prime numbers beginning with 3. After each repetition, the Fibonacci bits were tested to see if any ones remained and the program terminated when all the Fibonacci bits were zero, except for the three bits that corresponded to the known squares. This required the first 32 primes and was executed in six minutes. It should be pointed out that this method can only be used to demonstrate that a number is not a square, rather than proving that a number is a square. For example, if one of our Fibonacci numbers was of the form $1 + \prod_{n < N} p_n$ where p_n represents the n th prime number, its corresponding Fibonacci bit would remain a one for all primes less than N , and N would not have to be too large for this test to become unreasonable even for a very fast computer.

The author would like to express his appreciation to Dr. W. Macintyre who provided him with the free use of the facilities at the Computation Center of the University of Colorado and to Dr. L. Moser who first suggested the problem to the author.

University of Colorado
Boulder, Colorado

1. A. P. ROLLETT, "Advanced Problem No. 5080," *Amer. Math. Monthly*, February, 1963.
2. J. V. USPENSKY & M. A. HEASLET, *Elementary Number Theory*, McGraw-Hill, New York, 1939, Chapter X, Sect. 19; Chapter XI, Sect. 8.