SOME PROPERTIES ASSOCIATED WITH SQUARE FIBONACCI NUMBERS

JOHN H. HALTON
Brookhaven National Laboratory, Upton, Long Island, New York

1. INTRODUCTION

In 1963, both Moser and Carlitz [11] and Rollett [12] posed a problem.

Conjecture 1. The only square Fibonacci numbers are

$$F_0 = 0, \quad F_{-1} = F_1 = F_2 = 1, \quad \text{and} \quad F_{12} = 144 .$$

Wunderlich [14] showed, by an ingenious computational method, that for $3 \le m \le 1000008$, the only square F_m is F_{12}; and the conjecture was proved analytically by Cohn [5, 6, 7], Burr [2], and Wyler [15]; while a similar result for Lucas numbers was obtained by Cohn [6] and Brother Alfred [1].

Closely associated with Conjecture 1 is

Conjecture 2. When p is prime, the smallest Fibonacci number divisible by p is not divisible by p^2.

It is known (mostly from Wunderlich's computation) that Conjecture 2 holds for the first 3140 primes ($p \le 28837$) and for $p = 135721$, 141961, and 514229. Clearly, Conjecture 2, together with Carmichael's theorem (see [4], Theorem XXIII, and [9], Theorem 6), which asserts that, if $m \ge 0$, with the exception of $m = 1, 2, 6$, and 12, for each F_m there is a prime p, such that F_m is the smallest Fibonacci number divisible by p (whence F_m is not divisible by p^2 and so cannot be a square, if Conjecture 2 holds), implies Conjecture 1; but not vice versa. If Conjecture 2 holds, then the divisibility sequence theorem ([9], Theorem 1) can be strengthened to say that, if p is an odd prime and $n \ge 1$, then

$$\alpha(p,n) = p^{n-1}\alpha(p) . \tag{1}$$

In the notation of [9], Conjecture 2 for a given prime p states that $F_{\alpha(p)}$ is not divisible by p^2. This, by Lemma 8 and Theorem 1 of [9], is

*This work performed under the auspices of the U. S. Atomic Energy Commission.

The present paper is a revised version of a report written under auspices of the U. S. AEC while the author was at Brookhaven National Laboratory, Upton, L. I., N. Y. (Report No. AMD/384 BNL9300).

equivalent to

(2) $$\alpha(p^2) = p\alpha(p) \quad .$$

Since $\nu(p)$ is the highest power of p dividing $F_{\alpha(p)}$, this is equivalent to:

(3) $$\nu(p) = 1 \, .$$

By Lemma 11 of [9], p divides one and only one of F_{p-1}, F_p, and F_{p+1}, namely $F_{\lambda(p)}$, where $\lambda(p) = p - (5/p)$ and $(5/p)$ is the Legendre index. Thus, if $p \geq 5$, since $\lambda(p)$ is not divisible by p, while it is divisible by $\alpha(p)$, (2) is equivalent to

(4) $$F_{\lambda(p)} \text{ is not divisible by } p^2 \quad ,$$

and inspection of the cases $p = 2$, 3, and 5, shows that the equivalence holds for these primes also. Finally, (4) is equivalent to:

(5) $$F_{p-1}F_{p+1} \text{ is not divisible by } p^2 \quad .$$

This paper presents certain results obtained in the course of investigating the two Conjectures, the latter of which is still in doubt.

2. A THEOREM OF M. WARD

We begin with a theorem posed as a problem (published posthumously) by Ward [13]. A different proof from that given below was obtained independently by Carlitz [3].

Theorem A. Let

(6) $$\phi_n(x) = \sum_{s=1}^{n} x^s/s$$

and

$$k_p(x) = (x^{p-1} - 1)/p \;; \tag{7}$$

then, for any prime number $p \geq 5$, p^2 divides the smallest Fibonacci number divisible by p if and only if

$$\phi_{\frac{1}{2}(p-1)}\left(\frac{5}{9}\right) \equiv 2k_p\left(\frac{3}{2}\right) \pmod{p} \;. \tag{8}$$

Proof. We shall show that (8) is true if and only if (5) is false. We shall use the congruence (see [10], page 105) that, when $1 \leq t \leq p-1$,

$$\frac{t}{p}\binom{p}{t} \equiv (-1)^{t-1} \pmod{p} \;, \tag{9}$$

and Fermat's theorem (see [10], page 63), that

$$\text{if } (a,p) = 1, \quad a^{p-1} \equiv 1 \pmod{p} \;. \tag{10}$$

The identities

$$F_n = \frac{1}{\sqrt{5}}\left\{\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right\} \;, \tag{11}$$

$$F_{2n\pm1} = F_n^2 + F_{n\pm1}^2 \;, \tag{12}$$

$$F_{2n} = F_n(F_{n-1} + F_{n+1}) \;, \tag{13}$$

$$F_n^2 + (-1)^n = F_{n-1}F_{n+1} \;. \tag{14}$$

and

$$3F_n^2 + 2(-1)^n = F_{n-1}^2 + F_{n+1}^2 \;, \tag{15}$$

are well known (see [8], equations (3), (5), (64), (65), (67), and (95) with $m = 1$). From then it follows that (since $(1 \pm \sqrt{5})^2 = 2(3 \pm \sqrt{5})$)

$$\left(\frac{3}{2}\right)^n Q_n = \left(\frac{3}{2}\right)^n \left\{\left(1 + \frac{\sqrt{5}}{3}\right)^n + \left(1 - \frac{\sqrt{5}}{3}\right)^n\right\} = \left(\frac{1+\sqrt{5}}{2}\right)^{2n} + \left(\frac{1-\sqrt{5}}{2}\right)^{2n}$$

$$(16) \qquad = F_{4n}/F_{2n} = F_{2n-1} + F_{2n+1} = 2F_n^2 + F_{n-1}^2 + F_{n+1}^2$$

$$= 5F_n^2 + 2(-1)^n = 5F_{n-1}F_{n+1} - 3(-1)^n \quad .$$

Now, since $p > 5$, p is odd and $\frac{1}{2}(p - 1)$ is an integer. By (6) and (7), the factor $f = 6^p[\frac{1}{2}(p - 1)]!$ is prime to p and makes both $\phi_{\frac{1}{2}(p-1)}(5/9)$ and $k_p(3/2)$ into integers. Thus, modulo p, by (6), (9), (16), (7), and (10),

$$f\phi_{\frac{1}{2}(p-1)}\left(\frac{5}{9}\right) = 2f\sum_{s=1}^{\frac{1}{2}(p-1)} \frac{1}{2s}\left(\frac{\sqrt{5}}{3}\right)^{2s} = f\sum_{t=1}^{p-1}\frac{1}{t}\left\{\left(-\frac{\sqrt{5}}{3}\right)^t + \left(\frac{\sqrt{5}}{3}\right)^t\right\}$$

$$\equiv -\frac{f}{p}\sum_{t=1}^{p-1}\binom{p}{t}\left\{\left(\frac{\sqrt{5}}{3}\right)^t + \left(-\frac{\sqrt{5}}{3}\right)^t\right\} = -\frac{f}{p}(Q_p - 2)$$

$$= -\frac{f}{p}\left\{\left(\frac{2}{3}\right)^p (5F_{p-1}F_{p+1} + 3) - 2\right\}$$

$$= -5\cdot 4^p[\tfrac{1}{2}(p - 1)]!\,(F_{p-1}F_{p+1}/p) + f\left(\frac{2}{3}\right)^{p-1}\cdot 2k_p\left(\frac{3}{2}\right)$$

$$\equiv f\cdot 2k_p\left(\frac{3}{2}\right) - g(F_{p-1}F_{p+1}/p) \quad ,$$

where f and g are integers prime to p, and $F_{p-1}F_{p+1}/p$ is an integer. It follows that (8) is true if and only if $(F_{p-1}F_{p+1}/p) \equiv 0 \pmod p$, and this contradicts (5), proving the theorem.

3. ANOTHER CONJECTURE

We end the paper with an examination of a conjecture, which implies the first conjecture (known now to be true), in a rather different way from Conjecture 2. The underlying result is

Theorem B. Let p be a prime, and suppose that there exists a positive integer M, such that

(i) for no integer n, prime to p and greater than M, is F_m a square or p times a square; and

(ii) if n is positive and not greater than N, and F_n is a square or p times a square, then F_k is neither a square nor p times a square, when k is the least integer greater than M, such that k/n is a power of p;

then no F_m at all is a square or p times a square for $m > M$.

Proof. Suppose that (i) and (ii) hold, and that F_m is a square or p times a square. In contradiction of the theorem, let $m > M$. Then, by (i), m is divisible by p. Let $m = pm_1$, and write $F_m = AB^2C^2$, $F_{m_1} = BC^2D$, where D divides A and A is 1 or p. This makes F_m a square or p times a square, and divisible by F_{m_1}. Now, by the well-known identity (see [8, equation (35)], or [9], equation (8)])

$$F_m F_{m_1} = \sum_{h=1}^{p} \binom{p}{h} F_{m_1}^{h-1} F_{m_1-1}^{p-h} F_h \quad , \tag{17}$$

we get that

$$B(A/D) = BC^2D \sum_{h=2}^{p} \binom{p}{h} F_{m_1}^{h-2} F_{m_1-1}^{p-h} F_h + pF_{m_1-1}^{p-1}$$

Also, $(F_{m_1} - 1, F_{m_1}) = 1$, so B must divide p; that is, B is 1 or p; and again D is 1 or p. It follows that F_{m_1}, too, is a square or p times a square. Arguing similarly, we see that, if $m = p^r m_r$, then F_{m_r} is a square or p times a square. This will continue until $(m_s, p) = 1$, and then, by (i) $1 \leq m_s \leq M$. But then, by (ii), if $p^t m_s = m_{s-t}$ is the least such number greater than M, $s \geq t$, and $F_{m_{s-t}}$ cannot be a square or p times a square. This contradiction shows the correctness of the theorem.

Conjecture 3. There is no odd integer $m > 12$, such that F_m is a square or twice a square.

Theorem C. Conjecture 3 implies Conjecture 1.

Proof. Conjecture 3 states condition (i) of Theorem B, when $p = 2$ and $M = 12$. The only F_m, with $1 \leq m \leq 12$, which are squares or twice squares are $F_1 = F_2 = 1$, $F_3 = 2$, $F_6 = 8$, and $F_{12} = 144$. However, the corresponding F_k are $F_{16} = 3 \cdot 7 \cdot 47$ and $F_{24} = 2^5 \cdot 3^2 \cdot 7 \cdot 23$, and neither is a square or twice a square. Thus (ii) holds also, whence the conclusion of Theorem B, which includes Conjecture 1, is established.

4. PYTHAGOREAN RELATIONS

We close this paper by a rather closer examination of Conjecture 3, using the identities (12) and (13), with the well-known result, that the relation

$$x^2 + y^2 = z^2 \tag{18}$$

holds between integers if and only if there are integers s and t, mutually prime and of different parities, and an integer u, such that

$$x = (s^2 - t^2)u, \quad y = 2stu, \quad \text{and} \quad z = (s^2 + t^2)u \;. \tag{19}$$

Conjecture 3 leads us to examine the properties of Fibonacci numbers F_m, which are squares or twice squares, for odd integers m. We obtain the following rather remarkable results.

<u>Theorem D.</u> If m is odd, F_m is a square if and only if there are integers r, s, and t, such that $m = 12r \pm 1$, $s > t \geq 0$, s is odd, t is even, $(s,t) = 1$, and

$$F_{6r} = 2st, \qquad F_{6r\pm1} = s^2 - t^2 \;. \tag{20}$$

<u>Proof.</u> Since m is odd, put $m = 4n \pm 1$, determining n uniquely. Then, by (12),

$$F_m = F_{4n\pm1} = F_{2n}^2 + F_{2n\pm1}^2 \;. \tag{21}$$

Thus F_m is a square if and only if F_{2n}, $F_{2n\pm1}$, and $\sqrt{F_m}$ form a Pythagorean triplet. Since $(F_{2n}, F_{2n\pm1}) = 1$, $u = 1$, and this pair is $(s^2 - t^2)$ and 2st, while $F_{4n\pm1} = (s^2 \pm t^2)^2$. This gives that s and t are mutually prime and of different parities, with $s > t \geq 0$. By (12), $F_{2n\pm1} = F_n^2 + F_{n\pm1}^2$. Since $(F_n, F_{n\pm1}) = 1$, not both numbers are even, whence $F_{2n\pm1}$ is either odd or the sum of two odd squares, which must be of the form $8k + 2$. Since 2st is divisible by 4, it follows that

$$F_{2n} = 2st, \qquad F_{2n\pm1} = s^2 - t^2 \;. \tag{22}$$

Also, by (13), $2st = F_n(F_{n-1} + F_{n+1}) = F_n(2F_{n-1} + F_n)$. Since this must be divisible by 4, and $(F_n, 2F_{n-1} + F_n) = (F_n, 2)$, F_n must be even, so that $n = 3r$ (since $F_3 = 2$); whence $m = 12r \pm 1$, as stated in the theorem, and (22) becomes (20). Finally, $s^2 - t^2 = F_n^2 + F_{n-1}^2$ is of the form $4k + 1$, being the sum of an odd and an even square. Thus s must be odd and t even, as was asserted.

Since Conjecture 1 is valid, it follows from Theorem D that, if $r \geq 2$, the equations (20) are not satisfied by any integers r, s, and 6.

Theorem E. If m is odd, F_m is twice a square if and only if there are integers r, s, and t, such that $m = 12r \pm 3$, $s \geq t > 0$, s and t are both odd, $(s, t) = 1$, and

(23) $$F_{6r} = s^2 - t^2,\ F_{6r\pm3} = 2\,st\ .$$

Proof. We proceed much as for Theorem D. Let $m = 4n \pm 1$. Then, by (21), F_{2n} and $F_{2n\pm1}$ must both be odd (since they cannot both be even), so that $F_{2n\pm1}$ is even (since one out of every consecutive triplet of Fibonacci numbers, one is even, and its index is a multiple of 3). Thus $2n \pm 1 = 6r \pm 3$, whence $m = 12r \pm 3$, as stated in the theorem. It is easily verified that, since $2n = 6r \pm 2$ and $2n \pm 1 = 6r \pm 1$, and

(24) $$\begin{aligned} F_{6r+2} + F_{6r+1} &= F_{6r+3}, & F_{6r+2} - F_{6r+1} &= F_{6r}\ , \\ F_{6r-2} + F_{6r-1} &= F_{6r}, & F_{6r-2} - F_{6r-1} &= -F_{6r-3}\ . \end{aligned}$$

equation (21) yields that

(25) $$\begin{aligned} 2F_{12r\pm3} &= (F_{6r\pm2} + F_{6r\pm1})^2 + (F_{6r\pm2} - F_{6r\pm1})^2 \\ &= F_{6r}^2 + F_{6r\pm3}^2\ . \end{aligned}$$

Thus F_m is twice a square if and only if F_{6r}, $F_{6r\pm3}$, and $\sqrt{2F_{12r\pm3}}$ form a Pythagorean triplet. Clearly, since $F_3 = 2$ and $F_6 = 8$, F_{6r} is divisible by 8, but $F_{12r\pm3}$ and $F_{6r\pm3}$ are divisible by 2, but not by 4. Thus $u = 2$ and F_{6r} and $F_{6r\pm3}$ are of the forms $2(S^2 - T^2)$ and $4ST$, where $S > T \geq 0$, $(S, T) = 1$, and S and T are of opposite parities. In fact,

(26) $$F_{6r} = 4ST \text{ and } F_{6r\pm 3} = 2(S^2 - T^2) ,$$

since 4ST is clearly divisible by 8. Put $S + T = s$ and $S - T = t$; then (23) holds, and clearly $s \geq t \geq 0$, $(s,t) = 1$, and s and t are both odd, as stated in the theorem.

We finally note that Conjecture 3 holds if, for $r \geq 2$, the equations (23) are not satisfied by any integers r, s, and t.

REFERENCES

1. Brother U. Alfred, "On Square Lucas Numbers," The Fibonacci Quarterly, Vol. 2, (1964), pp. 11-12.
2. S. A. Burr, "On the Occurrence of Squares in Lucas Sequences," A. M. S. Notices (Abstract 63T-302) 10 (1963), p. 367.
3. L. Carlitz, Solution to Problem H-24, The Fibonacci Quarterly, Vol. 2, (1964) pp. 205-207.
4. R. D. Carmichael, "On the Numerical Factors of the Arithmetic Form $\alpha^n \pm \beta^n$," Ann. Math., Vol. 15 (1913-14), pp. 30-70.
5. J. H. E. Cohn, "On Square Fibonacci Numbers," Proc., 1963 Number Theory Conf. (Boulder, 1963), pp. 51-53.
6. J. H. E. Cohn, "Square Fibonacci Numbers, Etc.," The Fibonacci Quarterly, Vol. 2, (1964), pp. 109-113.
7. J. H. E. Cohn, "On Square Fibonacci Numbers," Jour. Lond. Math. Soc., Vol. 39, (1964), pp. 537-540.
8. J. H. Halton, "On a General Fibonacci Identity," The Fibonacci Quarterly, Vol. 3, (1965), pp. 31-43.
9. J. H. Halton, "On The Divisibility Properties of Fibonacci Numbers," The Fibonacci Quarterly, Vol. 4, (1966), Oct., pp. 217-240.
10. G. H. Hardy, E. M. Wright, An Introduction to the Theory of Numbers, (Clarendon Press, Oxford, 1962).
11. L. Moser, L. Carlitz, Problem H-2, The Fibonacci Quarterly, Vol. 1, No. 1, (Feb. 1963), p. 46.
12. A. P. Rollett, Problem 5080, Amer. Math. Monthly, Vol. 70, (1963), p. 216.
13. M. Ward, Problem H-24, The Fibonacci Quarterly, Vol. 1, No. 4, (Dec. 1963), p. 47.

14. M. Wunderlich, "On the Non-Existence of Fibonacci Squares," Math. Comp., Vol. 17 (1963), pp. 455-457.

15. O. Wyler, Solution to Problem 5080, Amer. Math. Monthly, Vol. 71, (1964), pp. 220-222.

* * * * *

The Fibonacci Bibliographical Research Center desires that any reader finding a Fibonacci reference send a card giving the reference and a brief description of the contents. Please forward all such information to:

Fibonacci Bibliographical Research Center,
Mathematics Department,
San Jose State College,
San Jose, California

* * * * *

PICKING AWAY AT 1967

CHARLES W. TRIGG

San Diego, California

1967 can be made from two 2's, three 3's, four 4's, five 5's, six 6's, or seven 7's with the aid of eighteen toothpicks and mixed Arabic and Roman number symbolism. That is,