FACTORIZATION OF FIBONACCI NUMBERS

D. E. DAYKIN
University of Malaya, Kuala Lampur
and
L. A. G. DRESEL
University of Reading, England

1. INTRODUCTION AND SUMMARY

The Fibonacci numbers F_n may be defined by the recurrence relation $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$ with $F_0 = 0$ and $F_1 = 1$. The factors of the first 60 Fibonacci numbers were published by Lucas (with only two errors) in 1877 [1], and recently a table of factors of F_n for $n \leq 100$ has been published by the Fibonacci Association in [2].

If F_z is the smallest Fibonacci number divisible by the prime p, then $z = z(p)$ is defined as the entry point (or rank) or p in the Fibonacci sequence; furthermore p divides F_n if and only if n is divisible by z(p), and there are rules for determining what power of p will divide such an F_n ([3], p. 396).

To find the entry point z(p) for a given p, we can generate the Fibonacci sequence modulo p until we obtain an element $F_z \equiv 0$; on a computer this process involves only additions and subtractions, and we work throughout with numbers less than 2p. Tables of entry points have been published by Brother U. Alfred [4], and have also been inverted to give p as a function of z. We extended the inverted table up to p = 660,000 by restricting our search to the first 256 Fibonacci numbers, i.e., to $z \leq 256$, and by this means we were able to give complete factorizations of 36 numbers F_n with $n > 100$ in [5].

In the present paper we shall adopt the alternative approach of fixing z and searching for primes for which this z is the entry point. In Sections 3 and 4 we shall prove the following theorems:

Theorem 1. If z is the entry point of a prime $p > 5$ then

(i) if z is odd, we have either

(a) $p = 4rz + 1$ and $p \equiv 1, 29, 41, 49 \pmod{60}$,

or (b) $p = (4r+2)z - 1$ and $p \equiv 13, 17, 37, 53 \pmod{60}$;

(ii) if $z \equiv 2 \pmod 4$, we have

$$p = rz + 1 \qquad \text{and} \qquad p = 1, 11, 19, 29 \pmod{30};$$

(iii) if $z \equiv 0 \pmod 4$, we have either

(a) $p = 2rz + 1$ and $p = 1, 29, 41, 49 \pmod{60}$,

or (b) $p = (2r + 1)z - 1$ and $p = 7, 23, 43, 47 \pmod{60}$,

where in all cases r is an integer.

Theorem 2. $2z(p)$ divides $p \pm 1$ if and only if $p \equiv 1 \pmod 4$.

In Section 5 we describe how we have used Theorem 1 as the basis of a computer program for factorizing Fibonacci numbers, and in Section 6 we give some numerical results obtained in this way.

2. SOME PRELIMINARY RESULTS

The Lucas numbers L_n are defined by the same recurrence relation as the Fibonacci numbers F_n, namely $L_n = L_{n-1} + L_{n-2}$ for $n \geq 2$, but with $L_0 = 2$ and $L_1 = 1$. We shall require the following well known identities:

$$F_{2n} = F_n L_n \tag{1}$$

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

$$L_n^2 - L_{n-1}L_{n+1} = (-1)^n 5 \ . \tag{3}$$

When p is an odd prime and m is an integer prime to p, the Legendre symbol (m/p) is defined to be $+1$ if m is a quadratic residue of p, i.e., if the equation

$$x^2 \equiv m \pmod p$$

has a solution in integers; whereas if there is no such solution, (m/p) is defined to be -1. It can be shown (ref. 6, Chap. 6) that, for $p > 5$,

$$(-1/p) = 1 \qquad \text{if and only if} \qquad p \equiv 1 \pmod 4 \tag{4}$$

(5a) $(5/p) = 1$ if and only if $p \equiv 1$ or $9 \pmod{10}$

(5b) $(5/p) = -1$ if and only if $p \equiv 3$ or $7 \pmod{10}$

(6) $(-5/p) = 1$ if and only if $p \equiv 1, 3, 7,$ or $9 \pmod{20}$.

It can also be shown (e.g., using Theorem 180, ref. 6), that if z is the Fibonacci entry point of p, then (for $p > 5$)

(7) $$p - (5/p) \equiv 0 \pmod{z} .$$

This leads to

Lemma 1

(8a) $$p = qz + 1 \quad \text{if} \quad p \equiv 1 \text{ or } 9 \pmod{10},$$

(8b) $$p = qz - 1 \quad \text{if} \quad p \equiv 3 \text{ or } 7 \pmod{10} ,$$

where z is the entry point of p and q is an integer.

We shall further use the fact that if p is a prime greater than 5, then

(9) $$p \equiv 1, 7, 11, 13, 17, 19, 23, \text{ or } 29 \pmod{30} ,$$

since otherwise p would be divisible by 2, 3, or 5.

If we reduce the Fibonacci sequence (for which $F_0 = 0$, $F_1 = 1$) modulo p, we obtain a periodic sequence. The period $k = k(p)$ is the smallest integer k for which

$$F_k \equiv 0 \pmod{p} \quad \text{and} \quad F_{k+1} \equiv 1 \pmod{p} .$$

It is clear that the entry point $z(p)$ will divide the period $k(p)$, and the following results have been proved by Oswald Wyler [7]:

(10a) $$k(p) = z(p) \quad \text{if} \quad z(p) \equiv 2 \pmod{4} ,$$

(10b) $$k(p) = 2z(p) \quad \text{if} \quad z(p) \equiv 0 \pmod{4} ,$$

(10c) $$k(p) = 4z(p) \quad \text{if} \quad z(p) \text{ is odd.}$$

We shall also use a result proved by D. D. Wall (ref. 8, Theorems 6 and 7), namely

(11a) $k(p)$ divides $p - 1$ if $p \equiv 1$ or $9 \pmod{10}$,

(11b) $k(p)$ divides $2(p + 1)$, but not $p + 1$, if $p = 3$ or $7 \pmod{10}$.

3. PROOF OF THEOREM 1

To prove Theorem 1 we have to consider separately the three cases of z odd, z twice an odd integer, and z divisible by 4, where $z = z(p)$ is the entry point of a prime $p > 5$.

(i) We first consider the case of z odd and prove

Lemma 2. If z is odd, then $p \equiv 1 \pmod 4$.

To prove this, take $n - 1 = z$ in the identity (2); then $n - 1$ is odd, and (by definition of z) p divides F_{n-1}, so that we have $(F_n)^2 \equiv -1$ (mod it follows, as stated in (4), that $p \equiv 1 \pmod 4$.

Combining this result with that of Lemma 1 we see that when z is odd we have either

(a) $p = 4rz + 1$ and $p \equiv 1$ or $9 \pmod{10}$,

or

(b) $p = (4r + 2)z - 1$ and $p \equiv 3$ or $7 \pmod{10}$.

Part (i) of Theorem 1, as stated in the introduction, then follows by using the result (9) and selecting those residues modulo 60 which satisfy $p \equiv 1 \pmod 4$.

(ii) Next, we consider the case where $z = 2s$ and s is an odd integer. In this case p divides F_{2s} but not F_s, so that it follows from the identity (1) that p divides L_s. Taking $n - 1 = s$ in the identity (3) we have $L_n^2 \equiv 5 \pmod p$, and it follows, as stated in (5a), that $p \equiv 1$ or $9 \pmod{10}$. Using this result together with Lemma 1 we obtain

Lemma 3. If z is twice an odd integer, then

$$p = qz + 1 \quad \text{and} \quad p \equiv 1 \text{ or } 9 \pmod{10} .$$

Part (ii) of Theorem 1 now follows by using the result (9). Moreover, Lemma 3 establishes the following result which was conjectured by A. C. Aitken (private communication to R. Rado in 1961):

Theorem 3. If p is a prime then $d \equiv 1 \pmod{p}$ for any divisor d of L_p.

(iii) Finally we consider the case where $z = 2s$ and s is an even integer. As before, it follows from (1) that p divides L_s, but taking $n - 1 = s$ in (3) we now obtain $L_n^2 \equiv -5 \pmod{p}$ since n is odd. Using the result (6) we deduce that $p \equiv 1, 3, 7$, or $9 \pmod{20}$, and combining this with Lemma with the result (9) we have that when $z \equiv 0 \pmod{4}$ either

$$\text{(a)} \qquad p = qz + 1 \quad \text{and} \quad p \equiv 1, 29, 41, 49 \pmod{60},$$

or

$$\text{(b)} \qquad p = qz - 1 \quad \text{and} \quad p \equiv 7, 23, 43, 47 \pmod{60}.$$

Since the result (10b) applies to these cases, the period k is now given by $k = 2z$. Applying (11a), we see that in case (a), q must be an even integer, say $q = 2r$. Similarly, applying (11b) we see that in case (b) q must be an odd integer, say $2r + 1$. This establishes part (ii) of Theorem 1.

In proving Theorem 1 we have used only the identities (1), (2) and (3). It is interesting to note that, although we applied similar techniques to many other identities, these did not lead to any further significant results.

4. PROOF OF THEOREM 2

To prove that for $p > 5$, $2z(p)$ divides $p - (5/p)$ if and only if $p \equiv 1 \pmod{4}$, we have to consider the three cases as before.

(i) When z is odd, we have by Lemma 2 that $p \equiv 1 \pmod{4}$; we also know from (7) that z divides $p - (5/p)$, which is an even number, and hence when z is odd $2z$ divides $p - (5/p)$.

(ii) When z is twice an odd integer, we have by Lemma 3 that

$$p = qz + 1 \quad \text{and} \quad p \equiv 1 \text{ or } 9 \pmod{10}.$$

It follows that $2z$ divides $p - 1$ if and only if q is even, and this condition is equivalent to $p \equiv 1 \pmod{4}$ in this case.

(iii) When $z \equiv 0 \pmod{4}$, we have already proved (at the end of Section 3) that either

(a) $p = qz + 1$ with q an even integer,

or

(b) $p = qz - 1$ with q an odd integer.

In case (a) we have $p \equiv 1 \pmod 4$ and $2z$ divides $p - 1$, whereas in case (b) we have $p \equiv 3 \pmod 4$ and $2z$ does not divide $p + 1$.

This completes the proof of Theorem 2.

A restricted form of this theorem, namely $2z(p)$ divides $p \pm 1$ if $p \equiv 1 \pmod 4$, has recently been proved by R. P. Backstrom ([9], lemmas 4 and 6).

5. APPLICATION TO THE FACTORIZATION OF FIBONACCI NUMBERS

Consider now the problem of finding the prime factors of F_n for a given n. If n is not prime, then F_n will have some improper factors p whose entry points z(p) divide n. Given n in the range $100 < n \leq 200$, it is a simple matter to consider all the divisors d of n and use the known factorizations of F_d for $d \leq 100$ (as given in [2]) to list all the improper factors of F_n. The remaining factors p will then be proper factors such that $z(p) = n$, and these must satisfy the conditions of Theorem 1 with $z = n$.

Consider first the case of n odd. Our computer program calculates F_n and then divides it in turn by all the improper factors of F_n (with suitable multiplicaties) which are supplied as data. We are then left with a quotient Q_n whose factors p must have $z(p) = n$. To determine these factors, we let the computer generate numbers N (not necessarily prime) satisfying the conditions for p in Theorem 1(i) with $z = n$. These numbers N in general fall into 8 residue classes modulo 60n, but it was found that when n is divisible by 3, 5, or 15 the number of residue classes goes up to 12, 10, or 15, respectively. For each n these residue classes were determined by the computer in accordance with Theorem 1 and the numbers N were then generated systematically from the lowest upward. For each N the program tests whether Q_n is divisible by N, and if it is it prints N as a factor and replaces Q_n by Q_n/N. Any factor N found in this way will be a prime, for if not, N would be the product of factors which should have been divided out from F_n or Q_n at an earlier stage of the progress. Finally, when N becomes sufficiently large for N^2 to exceed the current value of Q_n, we can stop the process and conclude that Q_n is prime; for if not, we would have $Q_n = N_1N_2 < N^2$ which implies that Q_n has a factor smaller than N, and any such factor would have been divided out at an earlier stage.

In the case of n even, say n = 2m, we can proceed slightly differently on account of the identity

$$F_{2m} = F_m L_m .$$

The computer program now generates L_m and our object is to factorize this. We need only supply as data those improper factors of F_n which do not also divide F_m, and dividing L_m by these factors we obtain the quotient Q_n. According as $\frac{1}{2}n = m$ is odd or even we use Theorem 1 (ii) or 1 (iii) to generate numbers N satisfying the conditions for p when z = n = 2m. It was found that these numbers N in general fall into 8, 10, or 12 residue classes modulo 30n, though in some cases 20 and even 30 residue classes occurred.

6. NUMERICAL RESULTS

A program on the lines described above was run on the Elliott 803 computer at Reading University, using multi-length integer arithmetic. In addition to the factorizations listed by us in [5], the following further factorizations were obtained (the factors before the asterisk being improper factors):

F103 = 519121 x 5644193 x 512119709
F115 = 5 x 28657 ⋆ 1381 x 2441738887963981
F133 = 13 x 37 x 113 ⋆ 3457 x 42293 x 351301301942501
F135 = 2 x 5 x 17 x 53 x 109 x 61 x 109441 ⋆ 1114769954367361
F141 = 2 x 2971215073 ⋆ 108289 x 1435097 x 142017737
F149 = 110557 x 162709 x 4000949 x 85607646594577

We also factorized a further 17 numbers F_n with n even, and because of the identity $F_{2m} = F_m L_m$ it will be sufficient to list the prime factors of the corresponding Lucas numbers L_m (those factors that are improper factors of F_{2m} are placed before the asterisk):

L61 = 5600748293801 (prime)
L62 = 3 * 3020733700601
L68 = 7 * 23230657239121
L71 = 688846502588399 (prime)
L73 = 151549 x 11899937029
L76 = 7 * 1091346396980401
L77 = 29 x 199 * 229769 x 9321929
L80 = 2207 * 23725145626561
L82 = 3 * 163 x 800483 x 350207569
L85 = 11 x 3571 * 1158551 x 12760031
L91 = 29 x 521 * 689667151970161
L92 = 7 * 253367 x 9506372193863
L93 = 2^2 x 3010349 * 63799 x 35510749
L94 = 3 * 563 x 5641 x 4632894751907
L96 = 2 x 1087 x 4481 * 11862575248703
L98 = 3 x 281 * 5881 x 61025309469041
L100 = 7 x 2161 * 9125201 x 5738108801

In each case the process was taken sufficiently far to ensure that the final quotient is a prime, as explained in the previous section. In the case of F115 this involved testing trial factors N almost up to 5×10^7.

REFERENCES

1. Edouard Lucas, Bull. di Bibl. e di St. d. Sc. Mat. e Fis., Vol. 10 (March 1877), pp. 129-170.
2. Brother U. Alfred, An Introduction to Fibonacci Discovery, The Fibonacci Association, 1965.
3. L. E. Dickson, History of the Theory of Numbers, Carnegie Institution, Vol. 1, 1919.
4. Brother U. Alfred, Tables of Fibonacci Entry Points, The Fibonacci Association, 1965.
5. L. A. G. Dresel and D. E. Daykin, "Factorization of 36 Fibonacci Numbers F_n with $n > 100$," Fibonacci Quarterly, Vol. 3, pp. 232-233, October, 1965.

[Continued on page 82.]