NOTE ON FIBONACCI PRIMALITY TESTING

John Brillhart
University of Arizona, Tucson, AZ 85721

(Submitted August 1996–Final Revision January 1997)

1. INTRODUCTION

One of the most effective ways of proving an integer N is prime is to show first that N is a probable prime, i.e., that $a^{N-1} \equiv 1$ (mod N) for some base a and $1 < a < N-1$, and then to find enough prime factors of $N \pm 1$ so that certain other conditions are satisfied (see [1] for details of such primality tests). The problem of finding these prime factors is, of course, the difficult and time-consuming part of this process, and anything that assists in the factoring of $N \pm 1$ is of great value, particularly when N is large.

In the case of the Fibonacci and Lucas numbers F_n and L_n, we are quite fortunate that identities exist whose form is exactly suited to this purpose. (These were discovered by Jarden [4, pp. 94-95]. Their use in primality testing was first made by the author in the early 1960's—see [4, p. 36].) The identities are all quite simple, asserting that $F_n \pm 1$ and $L_n \pm 1$ are equal to a product of certain Fibonacci and Lucas numbers with subscripts smaller than n, which numbers in turn may well have many known prime factors. Examples of these identities are:

$$F_{4k+1} - 1 = F_k L_k L_{2k+1} \quad \text{and} \quad F_{4k+1} + 1 = F_{2k+1} L_{2k}.$$

With the assistance of this set of identities, many large F_n's and L_n's have been identified as primes [2, p. 255].

In this note we give a collection of similar, but more complicated identities that can be used to establish the primality of the *primitive part* F_k^* of F_k, i.e., the cofactor remaining after the algebraic factors of F_k have been divided out. This cofactor is given by the formula (see [2, p. 252])

$$F_k^* = \prod_{d|k} F_d^{\mu(k/d)}, \ \mu \text{ the Möbius function.} \tag{1}$$

The subscript of F_k^* in the identities in the present collection has at most two distinct prime divisors, since an identity with three or more prime factors does not in general have a simple multiplicative structure on its right side, i.e., the right side is not just a ratio of products of F_k's and L_k's. The case of two prime divisors is transitional in that some identities have simple multiplicative structure and others do not [see (17) and (18)].

2. THE IDENTITIES

In the proofs that follow, we use elementary Fibonacci and Lucas identities. Also, throughout this note we use the familiar identity $F_{2r} = F_r L_r$ without further mention. In the first two theorems, the subscript of F_k^* is a power of a single prime.

Theorem 1: For $n \geq 3$,

$$F_{2^n}^* - 1 = \frac{L_{3 \cdot 2^{n-2}}}{L_{2^{n-2}}} \tag{2}$$

and

$$F^*_{2^n}+1=\frac{F_{3\cdot 2^{n-2}}}{F_{2^{n-2}}}. \tag{3}$$

Proof of (2): Substituting $r=2^{n-1}$ and $s=2^{n-2}$ into the identity

$$L_rL_s=L_{r+s}+(-1)^sL_{r-s}, \tag{4}$$

we obtain

$$F^*_{2^n}=\frac{F_{2^n}}{F_{2^{n-1}}}=L_{2^{n-1}}=\frac{L_{3\cdot 2^{n-2}}}{L_{2^{n-2}}}+1.$$

Proof of (3): Making the same substitution into the identity

$$F_sL_r=F_{r+s}-(-1)^sF_{r-s}, \tag{5}$$

we obtain

$$F^*_{2^n}=L_{2^{n-1}}=\frac{F_{3\cdot 2^{n-2}}}{F_{2^{n-2}}}-1.\ \square$$

Theorem 2: Let $p\equiv\varepsilon\pmod 4$ be a prime, where $\varepsilon=\pm1$. Then, for $n\geq1$,

$$F^*_{p^n}-1=\frac{F_{p^{n-1}(p-\varepsilon)/2}L_{p^{n-1}(p+\varepsilon)/2}}{F_{p^{n-1}}} \tag{6}$$

and

$$F^*_{p^n}+1=\frac{F_{p^{n-1}(p+\varepsilon)/2}L_{p^{n-1}(p-\varepsilon)/2}}{F_{p^{n-1}}}. \tag{7}$$

Proof of (6): If we substitute $r=p^{n-1}(\frac{p-\varepsilon}{2})$ and $s=p^{n-1}(\frac{p+\varepsilon}{2})$ into the identity

$$F_{r+s}=F_rL_s-(-1)^sF_{r-s}, \tag{8}$$

and use the fact that $F_{\varepsilon n}=F_n$ for n odd, then we obtain

$$F^*_{p^n}=\frac{F_{p^n}}{F_{p^{n-1}}}=\frac{F_{p^{n-1}(p-\varepsilon)/2}L_{p^{n-1}(p+\varepsilon)/2}}{F_{p^{n-1}}}+1.$$

Proof of (7): This follows in the same way by setting $r=p^{n-1}(\frac{p+\varepsilon}{2})$ and $s=p^{n-1}(\frac{p-\varepsilon}{2})$. □

Remarks:

1. For $p=3$, formulas (6) and (7) have a particularly nice form:

$$F^*_{3^n}-1=L^2_{3^{n-1}}\quad\text{and}\quad F^*_{3^n}+1=L_{2\cdot 3^{n-1}}. \tag{9}$$

2. For $p=5$, formulas (6) and (7) are of not interest here, since $F^*_{5^n}$, $n\geq2$, has 5 as an intrinsic factor [2, p. 252] and cannot be a prime. The numbers $F^*_{5^n}/5$ are dealt with in (26).

3. For $p=7$, formula (6) becomes the interesting formula

$$F^*_{7^n}-1=L_{7^{n-1}}L_{2\cdot 7^{n-1}}L_{3\cdot 7^{n-1}}. \tag{10}$$

4. In general, if $N=\frac{1}{2}(F^*_n\pm1)$ is a probable prime, then $N\mp1=\frac{1}{2}(F^*_n\mp1)$.

In the next theorems, the subscript of F_k^* has two different prime factors.

Theorem 3: Let q be an odd prime, then for $n \geq 1$,

$$F_{2q^n}^* - (-1)^{(q-1)/2} = \frac{5F_{q^{n-1}(q+1)/2}F_{q^{n-1}(q-1)/2}}{L_{q^{n-1}}} \tag{11}$$

and

$$F_{2q^n}^* + (-1)^{(q-1)/2} = \frac{L_{q^{n-1}(q+1)/2}L_{q^{n-1}(q-1)/2}}{L_{q^{n-1}}}. \tag{12}$$

Also, for $m \geq 2$, we have

$$F_{2^m q^n}^* - 1 = \frac{5F_{2^{m-1}q^{n-1}(q+1)/2}F_{2^{m-1}q^{n-1}(q-1)/2}}{L_{2^{m-1}q^{n-1}}} \tag{13}$$

and

$$F_{2^m q^n}^* + 1 = \frac{L_{2^{m-1}q^{n-1}(q+1)/2}L_{2^{m-1}q^{n-1}(q-1)/2}}{L_{2^{m-1}q^{n-1}}}. \tag{14}$$

Proof of (11): Substituting $r = q^{n-1}(\frac{q+1}{2})$ and $s = q^{n-1}(\frac{q-1}{2})$ into $L_{r+s} = 5F_rF_s + (-1)^s L_{r-s}$, we obtain

$$F_{2q^n}^* = \frac{F_{2q^n}F_{q^{n-1}}}{F_{q^n}F_{2q^{n-1}}} = \frac{L_{q^n}}{L_{q^{n-1}}} = \frac{5F_{q^{n-1}(q+1)/2}F_{q^{n-1}(q-1)/2}}{L_{q^{n-1}}} + (-1)^{(q-1)/2}.$$

Proof of (12): Making the same substitutions as in (11) into (4) leads to

$$F_{2q^n}^* = \frac{L_{q^n}}{L_{q^{n-1}}} = \frac{L_{q^{n-1}(q+1)/2}L_{q^{n-1}(q-1)/2}}{L_{q^{n-1}}} - (-1)^{(q-1)/2}.$$

Proof of (13) and (14): These results are obtained similarly by using $r = 2^{m-1}q^{n-1}(\frac{q+1}{2})$ and $s = 2^{m-1}q^{n-1}(\frac{q-1}{2})$ as in (11) and (12). □

Theorem 4: If $p < q$, p and q odd primes, then for $m, n \geq 1$,

$$F_{p^m q^n}^* - 1 = \frac{5F_{p^{m-1}q^{n-1}}F_{p^{m-1}q^{n-1}(q-1)}F_{p^{m-1}q^{n-1}(q+1)}}{F_{p^m q^{n-1}}} \cdot \sum_{r=0}^{\frac{p-3}{2}} \frac{(-1)^r p 5^{\frac{p-3}{2}-r}}{p-r} \binom{p-r}{r} \left\{ \frac{F_{p^{m-1}q^n}^{p-1-2r} - F_{p^{m-1}q^{n-1}}^{p-1-2r}}{F_{p^{m-1}q^n}^2 - F_{p^{m-1}q^{n-1}}^2} \right\}. \tag{15}$$

Proof: For brevity's sake, put $w = p^{n-1}q^{n-1}$. Then, using the formula (see [5, p. 209, (79)],

$$F_{pn} = \sum_{r=0}^{\frac{p-1}{2}} (-1)^r \frac{p}{p-r} \binom{p-r}{r} 5^{\frac{p-1}{2}-r} F_n^{p-2r}, \; n \text{ odd}, \tag{16}$$

we have that

$$
\begin{aligned}
&F_wF_{pqw}-F_{qw}F_{pw}\\
&=F_w\sum_{r=0}^{\frac{p-1}{2}}(-1)^r\frac{p}{p-r}\binom{p-r}{r}5^{\frac{p-1}{2}-r}F_{qw}^{p-2r}-F_{qw}\sum_{r=0}^{\frac{p-1}{2}}(-1)^r\frac{p}{p-r}\binom{p-r}{r}5^{\frac{p-1}{2}-r}F_w^{p-2r}\\
&=5F_{qw}F_w\sum_{r=0}^{\frac{p-3}{2}}(-1)^r\frac{p}{p-r}\binom{p-r}{r}5^{\frac{p-3}{2}-r}(F_{qw}^{p-1-2r}-F_w^{p-1-2r})\\
&=5F_{qw}F_w(F_{qw}^2-F_w^2)\sum_{r=0}^{\frac{p-3}{2}}(-1)^r\frac{p}{p-r}\binom{p-r}{r}5^{\frac{p-3}{2}-r}\left\{\frac{F_{qw}^{p-1-2r}-F_w^{p-1-2r}}{F_{qw}^2-F_w^2}\right\}.
\end{aligned}
$$

But, using the identity $F_{km}^2-(-1)^{k(m-1)}F_k^2=F_{k(m+1)}F_{k(m-1)}$ with $k=w$ and $m=q$, we have

$$
\begin{aligned}
&F_wF_{pqw}-F_{qw}F_{pw}\\
&=5F_{qw}F_wF_{w(q-1)}F_{w(q+1)}\sum_{r=0}^{\frac{p-3}{2}}(-1)^r\frac{p}{p-r}\binom{p-r}{r}5^{\frac{p-3}{2}-r}\left\{\frac{F_{qw}^{p-1-2r}-F_w^{p-1-2r}}{F_{qw}^2-F_w^2}\right\}.
\end{aligned}
$$

Thus,

$$
\begin{aligned}
F_{pqw}^*-1&=\frac{F_{pqw}F_w-F_{qw}F_{pw}}{F_{qw}F_{pw}}\\
&=\frac{5F_wF_{w(q-1)}F_{w(q+1)}}{F_{pw}}\sum_{r=0}^{\frac{p-3}{2}}(-1)^r\frac{p}{p-r}\binom{p-r}{r}5^{\frac{p-3}{2}-r}\left\{\frac{F_{qw}^{p-1-2r}-F_w^{p-1-2r}}{F_{qw}^2-F_w^2}\right\}.\ \square
\end{aligned}
$$

It is worth while to give some special cases.

Corollary 5: If q is a prime, then for $m,n\geq 1$,

$$F_{3^mq^n}^*-1=\frac{5F_{3^{m-1}q^{n-1}}F_{3^{m-1}q^{n-1}(q-1)}F_{3^{m-1}q^{n-1}(q+1)}}{F_{3^mq^{n-1}}},\ q\geq 5, \tag{17}$$

and for $q\geq 7$,

$$F_{5^mq^n}^*-1=\frac{25F_{5^{m-1}q^{n-1}}F_{5^{m-1}q^{n-1}(q-1)}F_{5^{m-1}q^{n-1}(q+1)}}{F_{5^mq^{n-1}}}(F_{5^{m-1}q^n}^2+F_{5^{m-1}q^{n-1}}^2-1). \tag{18}$$

The following are some further simple cases. Here q is a prime.

$$F_{3q}^*-1=\frac{5}{2}F_{q-1}F_{q+1},\ q\geq 5, \tag{19}$$

$$F_{5q}^*-1=5F_{q-1}F_q^2F_{q+1},\ q\geq 7, \tag{20}$$

and

$$F_{7q}^*-1=\frac{5}{13}F_{q-1}F_{q+1}(25F_q^4-10F_q^2+4),\ q\geq 11. \tag{21}$$

The next is a formula containing a "+1". From numerical evidence, there seem to be few identities with a "+" that have a right side with a multiplicative structure.

Theorem 6: If $q \geq 5$ is a prime, then

$$F_{3q}^* + 1 = \frac{L_{3q}}{2L_q}. \tag{22}$$

Proof: Using $F_{3r} = F_r(5F_r^2 + (-1)^r 3)$ and $L_{3r} = L_r(5F_r^2 + (-1)^r)$, we find that $L_q(F_{3q} + 2F_q) = L_q F_q(5F_q^2 - 3) + 2F_q L_q = F_q L_q(5F_q^2 - 1) = F_q L_{3q}$. Thus,

$$F_{3q}^* + 1 = \frac{F_{3q}}{F_3 F_q} + 1 = \frac{F_{3q} + 2F_q}{2F_q} = \frac{L_{3q}}{2L_q}. \quad \square$$

Some Examples: We consider the factorizations leading to proofs of the primality of the probable primes F_{145}^*, F_{2285}^*, and F_{14203}^*. In the first, we have

$$F_{145}^* = F_{5\cdot 29}^* = \frac{F_{145}}{F_5 F_{29}} = 3496199969307370798902 01.$$

Then, by (20) and Tables 2 and 3 in [2], we find the complete factorization:

$$\begin{aligned} F_{5\cdot 29}^* - 1 &= 5F_{28}F_{29}^2 F_{30} = 5(L_{14}L_7 F_7)F_{29}^2(L_{15}F_{15}) \\ &= 5(3\cdot 281\cdot 29\cdot 13)(514229^2)(2^2\cdot 11\cdot 31\cdot 2\cdot 5\cdot 61). \end{aligned}$$

In the second, identity (20) gives

$$\begin{aligned} F_{2285}^* - 1 = F_{5\cdot 457}^* - 1 &= 5F_{456}F_{457}^2 F_{458} \\ &= 5(L_{228}L_{114}L_{57}F_{57})F_{457}^2(L_{229}F_{229}), \end{aligned}$$

each factor of which is again completely factored using the tables in [2]. The primality of F_{145}^* and F_{2285}^* is established, respectively, from these complete factorizations using Theorem 1 in [1].

In the third, identity (21) is used to obtain

$$\begin{aligned} F_{14203}^* - 1 = F_{7\cdot 2029}^* - 1 &= \frac{5}{13}F_{2028}F_{2030}G \\ &= \frac{5}{13}(L_{1014}L_{507}F_{507})(L_{1015}F_{1015})G, \end{aligned}$$

where $G = 25F_{2029}^4 - 10F_{2029}^2 + 4$. As it happens, all the F_k's and L_k's can be factored completely and G is partially factored as $G = 7\cdot 2629093\cdot 47472487\cdot c$, where c is a 1682-digit composite cofactor. Since the logarithm of the product of the 64 known prime factors in these factorizations (counting multiplicity) is about 33.9% of the 2544-digit number F_{14203}^*, the "cube root" Theorem 5 in [1] can be used to establish the primality of this number. Fourteen of these factors have more than 20 digits.

For another example, see [3, §4], where (18) is used in the primality proof of the 1137-digit probable prime F_{7225}^*. A final example is the probable prime F_{4849}^*, for which not enough prime factors have been discovered to complete a primality proof. I would like to thank W. Keller for suggesting the above examples and for sending me information about them.

The next theorem deals with those F_n^*'s that have an intrinsic factor, which is divided out of the primitive part. Only the first power of an intrinsic factor can divide the primitive part.

Theorem 7: We have

$$\frac{F^*_{3\cdot 2^n}}{2} - 1 = \frac{1}{2} L_{2^{n-1}-1} L_{2^{n-1}+1}, \quad n \geq 2, \tag{23}$$

$$\frac{F^*_{3\cdot 2^n}}{2} + 1 = \prod_{k=1}^{n-1} F^*_{3\cdot 2^k} \quad n \geq 2, \tag{24}$$

$$\frac{F^*_{4\cdot 3^n}}{3} + 1 = \frac{1}{3} L^2_{2\cdot 3^{n-1}}, \quad n \geq 1, \tag{25}$$

$$\frac{F^*_{5^n}}{5} - 1 = 5F_{5^{n-1}-1} F^2_{5^{n-1}} F_{5^{n-1}+1}, \quad n \geq 2, \tag{26}$$

$$\frac{F^*_{8\cdot 7^n}}{7} + 1 = \frac{1}{7} L^2_{4\cdot 7^{n-1}} (L^4_{4\cdot 7^{n-1}} - 7L^2_{4\cdot 7^{n-1}} + 14), \quad n \geq 1. \tag{27}$$

Proof of (23) and (24): Using $L_{3r} = L_r(L_{2r} - (-1)^r)$ and $L_{2r} = L_r^2 - (-1)^r 2$, we have

$$F^*_{3\cdot 2^n} = \frac{F_{3\cdot 2^n} F_{2^{n-1}}}{F_{3\cdot 2^{n-1}} F_{2^n}} = \frac{L_{3\cdot 2^{n-1}}}{L_{2^{n-1}}} = L_{2^n} - 1 = L^2_{2^{n-1}} - 3. \tag{28}$$

Now, from $L_r^2 - (-1)^r 5 = L_{r-1} L_{r+1}$, we have $F^*_{3\cdot 2^n} - 2 = L^2_{2^{n-1}} - 5 = L_{2^{n-1}-1} L_{2^{n-1}+1}$, from which the identity follows.

Also, from the equalities in (28), we have

$$\begin{aligned}\frac{1}{2}(F^*_{3\cdot 2^n} + 2) &= \frac{1}{2}(L_{2^n} + 1) = \frac{1}{2}(L^2_{2^{n-1}} - 1) = \frac{1}{2}(L_{2^{n-1}} - 1)(L_{2^{n-1}} + 1) \\ &= \frac{1}{2}(L_{2^{n-1}} - 1)(L^2_{2^{n-2}} - 1) = \cdots = \frac{1}{2}(L_2^2 - 1)\sum_{k=2}^{n-1}(L_{2^k} - 1) = 4\sum_{k=2}^{n-1} F^*_{3\cdot 2^k} = \sum_{k=1}^{n-1} F^*_{3\cdot 2^k}.\end{aligned}$$

Proof of (25): Using $L_{3r} = L_r(L_r^2 - (-1)^r 3)$, we find that

$$F^*_{4\cdot 3^n} = \frac{F_{4\cdot 3^n} F_{2\cdot 3^{n-1}}}{F_{2\cdot 3^n} F_{4\cdot 3^{n-1}}} = \frac{L_{2\cdot 3^n}}{L_{2\cdot 3^{n-1}}} = L^2_{2\cdot 3^{n-1}} - 3,$$

which implies the result.

Proof of (26): From (16), we obtain the formula $F_{5r} = 5F_r(5F_r^4 - 5F_r^2 + 1)$, so

$$\frac{F^*_{5^n}}{5} - 1 = \frac{F_{5^n}}{5F_{5^{n-1}}} - 1 = 5F^2_{5^{n-1}}(F^2_{5^{n-1}} - 1) = 5F^2_{5^{n-1}} F_{5^{n-1}-1} F_{5^{n-1}+1},$$

using $F_r^2 + (-1)^r = F_{r-1}F_{r+1}$.

Proof of (27): From [4, p. 212, (86)],

$$L_{pn} = \sum_{r=0}^{\frac{p-1}{2}} (-1)^r \frac{p}{p-r}\binom{p-r}{r} L_n^{p-2r}, \quad n \text{ odd},$$

so $L_{7n} = L_n(L_n^6 - 7L_n^4 + 14L_n^2 - 7)$. Thus,

$$F^*_{8\cdot 7^n} = \frac{F_{8\cdot 7^n}F_{4\cdot 7^{n-1}}}{F_{4\cdot 7^n}F_{8\cdot 7^{n-1}}} = \frac{L_{4\cdot 7^n}}{L_{4\cdot 7^{n-1}}} = L^6_{4\cdot 7^{n-1}} - 7L^4_{4\cdot 7^{n-1}} + 14L^2_{4\cdot 7^{n-1}} - 7,$$

from which the identity follows. □

Remark: Numerical evidence suggests that, for $n \geq 2$, there are no multiplicative formulas for the even integers $N_1 = (F^*_{4\cdot 3^n}/3) - 1$ and $N_2 = (F^*_{5^n}/5) + 1$. On the other hand, if $\frac{1}{2}N_1$ or $\frac{1}{2}N_2$ should be probable primes, then the following formulas, which relate back to (24) and (25), might be useful in establishing their primality:

$$\frac{1}{2}N_1 + 1 = \frac{1}{2}\left(\frac{F^*_{4\cdot 3^n}}{2} + 1\right) \quad \text{and} \quad \frac{1}{2}N_2 - 1 = \frac{1}{2}\left(\frac{F^*_{5^n}}{5} - 1\right).$$

There are some other formulas involving F^*_n and L^*_n of various kinds, but these will not be considered here.

We conclude this note by observing that the identities used in the proofs, such as those in (4), (5), and (8), each contain the factor $(-1)^s$, which becomes the ± 1 in the identity for $F^*_n \pm 1$. In general Lucas sequences, of which the pair $\{F_n\}^\infty_{n=0}$ and $\{L_n\}^\infty_{n=0}$ is a special case, this factor is Q^s. Thus, the other Lucas sequences that have formulas like those in this note are those for which $|Q| = 1$ (see [1, p. 627]).

REFERENCES

1. J. Brillhart, D. H. Lehmer, & J. L. Selfridge. "New Primality Criteria and Factorizations of $2^m \pm 1$." *Math. of Comp.* **29.130** (1975):620-47.
2. J. Brillhart, P. L. Montgomery, & R. D. Silverman. "Tables of Fibonacci and Lucas Factorizations." *Math. of Comp.* **50.181** (1988):251-60; S1-S15.
3. H. Dubner & W. Keller. "New Fibonacci and Lucas Primes." *Math. of Comp.*, to appear.
4. D. Jarden. *Recurring Sequences.* 3rd ed. Jerusalem: Riveon Lematematika, 1973.
5. E. Lucas. "Théorie des fonctions numériques simplement périodiques." *Amer. J. Math.* **1.1** (1878):184-240; 289-321.

AMS Classification Numbers: 11A51, 11B39