MATHEMATICS OF COMPUTATION
Volume 68, Number 225, January 1999, Pages 417–427
S 0025-5718(99)00981-3

NEW FIBONACCI AND LUCAS PRIMES

HARVEY DUBNER AND WILFRID KELLER

ABSTRACT. Extending previous searches for prime Fibonacci and Lucas numbers, all probable prime Fibonacci numbers F_n have been determined for $6000 < n \leq 50000$ and all probable prime Lucas numbers L_n have been determined for $1000 < n \leq 50000$. A rigorous proof of primality is given for F_{9311} and for numbers L_n with $n = 1097$, 1361, 4787, 4793, 5851, 7741, 10691, 14449, the prime L_{14449} having 3020 digits. Primitive parts F_n^* and L_n^* of composite numbers F_n and L_n have also been tested for probable primality. Actual primality has been established for many of them, including 22 with more than 1000 digits. In a Supplement to the paper, factorizations of numbers F_n and L_n are given for $n > 1000$ as far as they have been completed, adding information to existing factor tables covering $n \leq 1000$.

1. INTRODUCTION

Fibonacci numbers F_n and the related Lucas numbers L_n are defined recursively by the formulas

$$\begin{aligned} F_{n+2} &= F_{n+1} + F_n, \qquad n \geq 0, \qquad F_0 = 0, \quad F_1 = 1, \\ L_{n+2} &= L_{n+1} + L_n, \qquad n \geq 0, \qquad L_0 = 2, \quad L_1 = 1. \end{aligned}$$

These numbers have many interesting properties and applications; see [7] and the historical references therein. Here we report on a search for new primes F_n and L_n which extends previous work of J. Brillhart, H. C. Williams, and F. Morain.

It turned out that F_n is a prime (or a probable prime, when marked with an asterisk) for $n = 3$, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47, 83, 131, 137, 359, 431, 433, 449, 509, 569, 571, 2971, 4723, 5387, 9311, 9677*, 14431*, 25561*, 30757*, 35999*, 37511*, and for no other $n \leq 50000$. The interval $n \leq 1000$ had been covered by Brillhart; cf. the review of [7]. Williams searched $1000 < n \leq 6000$ for probable primes (as reported by Brillhart [2]) and showed that F_{2971} was indeed a prime, while F_{4723} and F_{5387} were subsequently proven prime by Morain [12] using techniques similar to those we will be describing below.

Also, L_n has been shown to be a prime (or a probable prime) for $n = 0$, 2, 4, 5, 7, 8, 11, 13, 16, 17, 19, 31, 37, 41, 47, 53, 61, 71, 79, 113, 313, 353, 503, 613, 617, 863, 1097, 1361, 4787, 4793, 5851, 7741, 8467*, 10691, 12251*, 13963*, 14449, 19469*, 35449*, 36779*, 44507*, and for no other $n \leq 50000$. The interval $n \leq 500$ had been covered by Brillhart [7] and was extended to $n \leq 1000$ by Williams (as mentioned in [2]), who found four new primes L_n.

Received by the editor March 29, 1996 and, in revised form, April 10, 1997.
1991 *Mathematics Subject Classification.* Primary 11A51; Secondary 11B39, 11–04.
Key words and phrases. Fibonacci numbers, Lucas numbers, primality testing, large primes, prime primitive parts, factor tables.

We recall that F_n with $n \geq 5$ cannot be prime unless n itself is a prime. Also, L_n with $n > 0$ can be prime only when n is a prime or a power of 2. For large numbers F_n and L_n, rigorous proofs of primality became possible due to the multiplicative structure of $F_n \pm 1$ and $L_n \pm 1$, the existence of extensive factor tables, and the availability of powerful factoring algorithms.

2. Primality testing

The theorems applied to prove primality of large numbers N rely on the provision of a completely factored part of $N-1$ or of $N+1$ that exceeds in magnitude $N^{1/2}$ or lies, at least, between $N^{1/3}$ and $N^{1/2}$. We first state the theorems, which are derived from those found in [4], and then we discuss their application from a practical point of view.

Let $N - 1 = G \cdot H$, where G is a completely factored portion of $N - 1$, $H > 1$, and $(G, H) = 1$.

Theorem 1. *Suppose $G^2 > N$. If for each prime p_i dividing G there exists an a_i such that $a_i^{N-1} \equiv 1 \pmod{N}$ and $(a_i^{(N-1)/p_i} - 1, N) = 1$, then N is prime.*

Theorem 2. *Suppose $2G^3 > N$. Let r and s be defined by $H = 2Gs + r$, $1 \leq r < 2G$, where $s = 0$ or otherwise $r^2 - 8s$ is not a perfect square. If for each prime p_i dividing G there exists an a_i such that $a_i^{N-1} \equiv 1 \pmod{N}$ and $(a_i^{(N-1)/p_i} - 1, N) = 1$, then N is prime.*

A pair of Lucas sequences $\{U_n\}$, $\{V_n\}$ is defined by the formulas

$$\begin{aligned} U_{n+2} &= PU_{n+1} - QU_n, \qquad n \geq 0, \qquad U_0 = 0, \qquad U_1 = 1, \\ V_{n+2} &= PV_{n+1} - QV_n, \qquad n \geq 0, \qquad V_0 = 2, \qquad V_1 = P, \end{aligned}$$

where P and Q are integers such that the discriminant $D = P^2 - 4Q \neq 0$. Note that the Fibonacci and Lucas numbers we are studying in this paper are included in the more general definition by assuming $P = 1$, $Q = -1$, $D = 5$.

Now let $N + 1 = G \cdot H$, where G is a completely factored portion of $N + 1$, $H > 1$, and $(G, H) = 1$.

Theorem 3. *Suppose $(G-1)^2 > N$. If for each prime p_i dividing G there exists a Lucas sequence $\{U_n^{(i)}\}$ with a given discriminant D such that $(D/N) = -1$, $U_{N+1}^{(i)} \equiv 0 \pmod{N}$, and $(U_{(N+1)/p_i}^{(i)}, N) = 1$, then N is prime.*

Theorem 4. *Suppose $(G-1)^3 > N$. Let r and s be defined by $H = 2Gs + r$, $|r| < G$, where $s = 0$ or otherwise $r^2 - 8s$ is not a perfect square. If for each prime p_i dividing G there exists a Lucas sequence $\{U_n^{(i)}\}$ with a given discriminant D such that $(D/N) = -1$, $U_{N+1}^{(i)} \equiv 0 \pmod{N}$, and $(U_{(N+1)/p_i}^{(i)}, N) = 1$, then N is prime.*

Theorems 2 and 4 are corollaries to Theorems 5 and 17 of [4] obtained by letting $m = 1$ in the assumptions of both theorems, which seems to be a good choice for most practical purposes. Note that, in Theorem 2, $s = 0$ would mean $H = r$ and $H < 2G$, the inequality being equivalent to $N - 1 = G \cdot H < 2G^2$ or $N \leq 2G^2$. Thus, the square root of $r^2 - 8s$ must be calculated whenever $2G^3 > N > 2G^2$, and this is always the case when G scarcely exceeds $(N/2)^{1/3}$. Similarly, in Theorem 4, $s = 0$ means $N \leq G^2 - 2$ and the square root must be calculated when $(G-1)^3 > N > G^2 - 2$.

Examining Theorem 1 and Theorem 2, it is apparent in both cases that the amount of computation needed to prove a number N prime is roughly proportional to the number of (different) prime factors p_i of the completely factored part.

Now, suppose we have a factored part $G > N^{1/2}$ that includes many small factors p_i while the larger ones alone suffice to surpass the minimum limit of $(N/2)^{1/3}$. In this situation it appears more advisable to use Theorem 2 with a reduced set of factors, though at first sight we would be inclined to apply Theorem 1. The reason is that for every small p_i discarded the computation of at least one power modulo N is saved. The required additional computation of a single square root can certainly be neglected.

It is interesting to note that the absence of small factors p_i in the used factored part of $N-1$ has another favorable effect. In this case, usually a single base a fixed in advance is sufficient to check all the conditions guaranteeing primality. In particular, the power $a^{N-1} \bmod N$ has to be calculated only once for all the larger p_i involved.

In the experience of the first author in determining very large primes over many years, this has in fact been the standard situation, which allows a further important shortcut. If $A = a^H \bmod N$ is computed first, then $a^{N-1} \equiv A^G \pmod N$ and $a^{(N-1)/p_i} \equiv A^{G/p_i} \pmod N$ for each p_i. This eliminates about two thirds of the computing time otherwise needed.

In Section 4 our general observations will be illustrated by a 1137-digit prime N. Considerations similar to the above suggest that, whenever possible, also Theorem 4 should be preferred to Theorem 3 on the same grounds.

3. Application to Fibonacci and Lucas numbers

In the specific case of proving primality for Fibonacci and Lucas numbers we can try to obtain a sufficiently large factored part by using the following identities and relations, which are all taken from [5], the most relevant reference for this paper. We include them here to make our exposition largely self-contained. The basic relations are:

$$\begin{aligned}
F_{4k+1} - 1 &= F_k L_k L_{2k+1}, & F_{4k+3} - 1 &= F_{k+1} L_{k+1} L_{2k+1},\\
F_{4k+1} + 1 &= F_{2k+1} L_{2k}, & F_{4k+3} + 1 &= F_{2k+1} L_{2k+2},\\
L_{4k+1} - 1 &= 5 F_k L_k F_{2k+1}, & L_{4k+3} - 1 &= L_{2k+1} L_{2k+2},\\
L_{4k+1} + 1 &= L_{2k} L_{2k+1}, & L_{4k+3} + 1 &= 5 L_{k+1} F_{k+1} F_{2k+1}.
\end{aligned}$$

To obtain the needed factorizations of Fibonacci and Lucas numbers appearing on the right-hand side of each identity, use is made of the following facts. First, we recall that $F_{2n} = F_n L_n$. Thus every F_n with n even always splits into the product of an F_n with odd subscript n and one or more factors L_n.

A Fibonacci number F_n with n odd is algebraically factored as

$$F_n = \prod_{d|n} F_d^*, \quad n \geq 1, \quad \text{where} \quad F_d^* = \prod_{\delta|d} F_\delta^{\mu(d/\delta)}, \quad d \geq 1,$$

μ being the Möbius function. F_n^* is called the primitive part of F_n. The algebraic multiplicative structure of L_n is described similarly. Let $n = 2^s m$, where m is odd. Then

$$L_n = \prod_{d|m} L_{2^s d}^*, \quad n \geq 1, \quad \text{where} \quad L_{2^s d}^* = \prod_{\delta|d} L_{2^s \delta}^{\mu(d/\delta)}, \quad d \geq 1.$$

Now L_n^* is the primitive part of L_n.

4. The primality of L_{14449}

To exemplify various aspects of the methodology, we give a rather detailed analysis of the 3020-digit Lucas number L_{14449}. In this case we have $14449 = 4 \cdot 3612 + 1$ and

$$L_{14449} - 1 = 5F_{3612}L_{3612}F_{7225},$$

where the last factor is

$$F_{7225} = F_5^* F_{17}^* F_{25}^* F_{85}^* F_{289}^* F_{425}^* F_{1445}^* F_{7225}^*.$$

Surprisingly enough, F_{7225}^* is a 1137-digit probable prime representing 37.6% of the digits of $L_{14449} - 1$. If we could prove F_{7225}^* prime, then Theorem 2 would provide a primality proof for the given Lucas number.

To accomplish this, the clue was given by the following formula kindly supplied by J. Brillhart [2], namely,

$$F_{25p^2}^* - 1 = 25F_{5p}F_{5p(p-1)}F_{5p(p+1)}(F_{5p^2}^2 + F_{5p}^2 - 1)/F_{25p}.$$

For $p = 17$, $25p^2 = 7225$, this becomes

$$F_{7225}^* - 1 = 25F_{85}F_{1360}F_{1530}(F_{1445}^2 + F_{85}^2 - 1)/F_{425} = G \cdot H,$$

where

$$G = 5F_{1360}F_{1530} = 5F_{85}L_{85}L_{170}L_{340}L_{680}F_{765}L_{765}$$

and

$$H = 5F_{85}(F_{1445}^2 + F_{85}^2 - 1)/F_{425} = 7 \cdot 43 \cdot 3407 \cdot 7639 \cdot \text{c524}.$$

The complete factorization of the portion G, which has 604 digits, is obtained by joining the prime factors of

$$\begin{aligned} L_{680}^* &= 1376321 \cdot 9830081 \cdot 280381350009601 \\ &\quad \cdot 2843304747267841 \cdot 616713904085105580641 \cdot \text{p44}, \\ L_{765}^* &= 1531 \cdot 852211 \cdot 609198772474674177793102772460 1 \cdot \text{p41} \end{aligned}$$

to those of all the remaining components which are factored in [5]. Altogether, the portion G has about 53.1% of the number of digits of $F_{7225}^* - 1$ and contains 65 different prime factors p_i to be taken into account if Theorem 1 were to be applied to prove the primality of F_{7225}^*.

As we have indicated in Section 2, the amount of computation involved might be reduced by neglecting the 16 small divisors p_i of G having $p_i < 1000$. Then the remaining part of G still has 50.6% of the total number of digits. However, the reduction is much more substantial if we choose to use Theorem 2 instead. Retaining only those 17 prime factors p_i of G having 14 digits at least (the largest one has 56 digits), their product gives a 400-digit number representing a 35.1% portion of $F_{7225}^* - 1$, well in excess of the required minimum.

Once the proof is complete, the primality of the 3020 digit number L_{14449} can also be established.

A similar but less fortunate situation occurred with the probable prime number F_{35999}, since

$$F_{35999} - 1 = F_{9000}L_{9000}L_{17999},$$

$$L_{17999} = L_{41}^* \cdot L_{439}^* \cdot L_{17999}^*,$$

TABLE 1. Summary of primality proofs for new Fibonacci and Lucas primes

Factored number	Number of digits	Factored portion	Number of factors used	Digits of least factor used
$F_{9311}-1$	1946	0.386	31	8
$L_{1097}-1$	230	1.000	3	29
$L_{1361}-1$	285	1.000	3	34
$L_{4787}-1$	1001	0.530	4	18
$L_{4793}+1$	1002	0.714	1	475
$L_{5851}-1$	1223	0.557	13	16
$L_{7741}-1$	1618	0.586	9	28
$L_{10691}+1$	2235	0.347	37	4
$L_{14449}-1$	3020	0.662	1	1137

and

$$L^*_{17999} = 35999 \cdot 615492974061 \cdot \text{prp3645},$$

the prp3645 cofactor G of L^*_{17999} representing 48.4% of the number $F_{35999}-1$. Trying to factor $G-1$ or $G+1$ is a hopeless enterprise, as an algebraic decomposition cannot be expected and the magnitude of the number is prohibitive anyway. Unfortunately, the portion $F_{9000}L_{9000}$ did not supply the factors needed for a prime-proof of F_{35999} either.

For the one Fibonacci number and several Lucas numbers N whose primality could be established for the first time, we give in Table 1 their number of digits, the proportion of the effectively factored part G of $N-1$ or $N+1$, which is approximately $\log(G)/\log(N)$, and the number of factors sufficient to apply Theorem 2 or Theorem 4. Finally, the size of the least factor included is shown.

5. Prime primitive parts

Encouraged by the conclusive treatment of F^*_{7225} and by a remark in [5] saying that there are a number of additional formulas breaking the factorization of $F^*_n \pm 1$ and $L^*_n \pm 1$ into factorizations of smaller numbers F_n and L_n, we engaged in a systematic search for prime primitive parts. Let us first summarize our findings, including earlier knowledge from [5].

For composite Fibonacci numbers F_n, the primitive part F^*_n has been shown to be a prime (or a probable prime, when marked with an asterisk) for $n = 9$, 15, 21, 33, 35, 39, 45, 51, 63, 65, 75, 93, 105, 111, 119, 121, 123, 135, 145, 185, 195, 201, 207, 209, 225, 231, 235, 245, 285, 287, 299, 301, 321, 335, 363, 399, 423, 453, 473, 693, 707, 771, 1047, 1113, 1215, 1365, 1371, 1387, 1533, 1537, 1539, 2185, 2285, 2289, 2361, 2511, 2587, 2733, 2877, 3211, 3339, 3757, 3857, 3867, 3927, 4025, 4849*, 4881, 5141*, 5579, 5691, 5921*, 6285, 6705, 7035, 7225, 7397*, 7423*, 7783*, 7787*, 7917, 8225*, 8275, 8283*, 8917*, 9499*, 9813, 10025, 10203*, 10215*, 10377, 11457*, 11545, 11915, 12137*, 12717, 12987*, 13797*, 13893*, 13995*, 14203, 16225*, 16745*, 17221*, 18689*, 19415*, and for no other $n \le 20000$.

For composite Lucas numbers L_n, the primitive part L_n^* has been shown to be a prime (or a probable prime) for $n = 9$, 10, 14, 15, 20, 21, 26, 27, 30, 33, 36, 38, 49, 56, 62, 66, 68, 70, 72, 76, 78, 80, 86, 90, 91, 110, 117, 120, 121, 136, 140, 144, 164, 168, 172, 178, 202, 207, 220, 261, 284, 328, 354, 357, 420, 423, 458, 459, 468, 480, 504, 513, 530, 586, 606, 630, 633, 636, 644, 679, 812, 836, 837, 861, 914, 966, 999, 1082, 1098, 1178, 1257, 1306, 1318, 1326, 1431, 1450, 1504, 1558, 1617, 1632, 1671, 1742, 1767, 1863, 1881, 2013, 2057, 2058, 2091, 2170, 2220, 2270, 2279, 2307, 2400, 2944, 2946, 2973, 3069, 3074, 3106, 3248, 3510, 3753, 3777, 4006, 4152, 4200, 4558*, 4627, 5007, 5048, 5064, 5160, 5371*, 5414, 5496, 5498, 5574, 5656, 5707*, 6028*, 6044, 6594, 6651, 6750, 6958*, 6973*, 7116, 7370*, 8777*, 8781, 8827*, 9072, 9356, 9683*, 9996*, 10500*, 10514*, 10821, 11140*, 11221, 11662*, 11808, 11836*, 12190*, 13173, 13876, 14241*, 14318*, and for no other $n \leq 15000$.

As we could not find the formulas alluded to in the published literature, we independently developed some identities which proved useful for establishing the primality of primitive parts F_n^* and L_n^* in quite a number of cases.

Let us assume that the index n is of the particular form $n = q^r p$, where q, p are primes, $q \leq 5$, p odd, $p \neq q$, and $r \geq 1$. Then we have:

$$L^*_{2^r p} - 1 = 5F_{2^{r-1}(p-1)}F_{2^{r-1}(p+1)}/L_{2^r},$$

$$L^*_{3^r p} - 1 = 5F_{3^{r-1}(p-1)}F_{3^{r-1}(p+1)}/(L_{2\cdot 3^{r-1}} + 1),$$

$$F^*_{3^r p} - 1 = 5F_{3^{r-1}(p-1)}F_{3^{r-1}(p+1)}/(L_{2\cdot 3^{r-1}} - 1),$$

$$F^*_{5^r p} - 1 = 5F_{5^{r-1}(p-1)}F_{5^{r-1}(p+1)}\frac{L_{5^{r-1}(p-1)}L_{5^{r-1}(p+1)} - 1}{L_{4\cdot 5^{r-1}} - L_{2\cdot 5^{r-1}} + 1}.$$

For the particular case of $r = 1$ each of these formulas boils down to a very simple form:

$$L^*_{2p} - 1 = (5/3)F_{p-1}F_{p+1},$$

$$L^*_{3p} - 1 = (5/4)F_{p-1}F_{p+1},$$

$$F^*_{3p} - 1 = (5/2)F_{p-1}F_{p+1},$$

$$F^*_{5p} - 1 = 5F_{p-1}F_{p+1}F_p^2.$$

The last of these expressions follows from the fact that $(L_{p-1}L_{p+1}-1)/5 = F_p^2$. This relation, as well as the given general formulas, can be verified through calculation involving the well-known expressions of F_n and L_n in terms of $\alpha = (1+\sqrt{5})/2$ and $\beta = (1-\sqrt{5})/2$.

Since p is assumed to be odd, on the right-hand side we always have a decomposition of the form

$$F_{p-1}F_{p+1} = F_{(p-1)/2}L_{(p-1)/2}F_{(p+1)/2}L_{(p+1)/2},$$

which similarly applies to the general case. This further facilitates finding the prime factors needed to invoke Theorem 2.

6. The primality of L^*_{13876}

Again, let us first discuss an instructive particular case. For the 2900-digit number L^*_{13876} we have $13876 = 2^2 \cdot 3469$, where 3469 is a prime, and thus we obtain the decomposition

$$L^*_{13876} - 1 = 5F_{2\cdot 3468}F_{2\cdot 3470}/L_4$$

$$= (5/7)F_{867}L_{867}L_{1734}L_{3468}F_{1735}L_{1735}L_{3470},$$

observing that L_{289} divides L_{867}, L_{102} and L_{578} divide L_{1734}, L_{204} divides L_{3468}, F_{347} divides F_{1735}, and L_{694} divides L_{3470}. Also, $L_{1735} = L_{347} \cdot A_{1735} \cdot B_{1735}$ (for this special Aurifeuillian factorization, see [5]).

The numbers F_{867}, L_{289}, L_{102}, L_{204}, F_{347}, and L_{347} were factored in [5]. Moreover, we factored

$$A_{1735} = 11 \cdot 17351 \cdot 4202171 \cdot 140916701 \cdot 3124791659551720658921 \cdot \text{p104},$$
$$B_{1735} = 14719741 \cdot 88704249076841 \cdot 2349072345221377801 \cdot \text{p87},$$

as well as

$$L_{578} = 3 \cdot 67 \cdot 3467 \cdot 63443 \cdot 893346576820363 \cdot 52117518727310243 \cdot \text{p79},$$
$$L_{694} = 3 \cdot 594273587 \cdot 27159850749888907 \cdot 61443319601189051182963 \cdot \text{p97}.$$

Seeking for more of the needed prime factors, we also found

$$L^*_{1156} = 6452026727 \cdot 55920023657924567 \cdot \text{c201},$$
$$L^*_{1734} = 521511493561 \cdot 8030487401843243 \cdot \text{c200},$$
$$F^*_{1735} = 97382081 \cdot 4765843741 \cdot 2344355547421 \cdot \text{c260},$$

the first of these primitive parts dividing L_{3468}.

With all these factors at hand, we could proceed to prove the primality of L^*_{13876}. Multiplying the 37 known prime factors of $L^*_{13876} - 1$ having 8 digits at least, we got a portion of 999 digits, or 34.4%, sufficient to apply Theorem 2. The final test took about 21 minutes on the special purpose computer designed by the first author and described in [6].

It seems worth mentioning that this not only completed our primality proof, but also the remarkable factorization of the Lucas number $L_{13876} = L^*_4 L^*_{13876} = 7L^*_{13876}$.

The summary of Table 2 is an analogue to Table 1 for prime primitive parts with more than 1000 digits. The recorded form of subscripts shows in which cases the formulas of the last section could be applied successfully. For the primes F^*_{14203} and L^*_{11221}, whose subscripts are of the form $7^r p$, and for those three instances where the subscript has more than two different prime factors, see the next short section on more recent developments in the field.

The given formulas were also applicable to F^*_n for $n = 2285$ $(= 5 \cdot 457)$, 2361 $(= 3 \cdot 787)$, 2511 $(= 3^4 \cdot 31)$, 2733 $(= 3 \cdot 911)$, 3867 $(= 3 \cdot 1289)$, 4881 $(= 3 \cdot 1627)$, and to L^*_n for $n = 2944$ $(= 2^7 \cdot 23)$, 3106 $(= 2 \cdot 1553)$, 3753 $(= 3^3 \cdot 139)$, 3777 $(= 3 \cdot 1259)$, 4006 $(= 2 \cdot 2003)$, 5007 $(= 3 \cdot 1669)$, 6651 $(= 3^2 \cdot 739)$.

A number of primitive parts that resisted such a concise treatment, but were of a size just accessible to a general prime-proving procedure, have been subjected to APRT-CL, the Cohen-Lenstra version of the Adleman-Pomerance-Rumely test implemented in [13]. The largest prime primitive part confirmed in this way was the 843-digit number F^*_{7917}, which consumed 134 hours and 28 minutes on a Pentium 100 processor.

TABLE 2. Summary of primality proofs for primitive parts F_n^* and L_n^* with more than 1000 digits

Factored number	Form of subscript	Number of digits	Factored portion	Number of factors used
$F_{7225}^* - 1$	$5^2 \cdot 17^2$	1137	0.540	17
$F_{8275}^* - 1$	$5^2 \cdot 331$	1380	0.499	31
$F_{9813}^* - 1$	$3 \cdot 3271$	1367	0.469	13
$F_{10025}^* - 1$	$5^2 \cdot 401$	1672	0.434	23
$F_{10377}^* - 1$	$3^2 \cdot 1153$	1445	0.441	19
$F_{11545}^* - 1$	$5 \cdot 2309$	1930	0.500	9
$F_{11915}^* - 1$	$5 \cdot 2383$	1992	0.369	13
$F_{12717}^* - 1$	$3^4 \cdot 157$	1761	0.397	35
$F_{14203}^* - 1$	$7 \cdot 2029$	2544	0.336	49
$L_{5048}^* - 1$	$2^3 \cdot 631$	1054	0.565	16
$L_{5414}^* - 1$	$2 \cdot 2707$	1131	0.475	8
$L_{5498}^* - 1$	$2 \cdot 2749$	1149	0.535	8
$L_{5656}^* - 1$	$2^3 \cdot 7 \cdot 101$	1004	0.337	42
$L_{6044}^* - 1$	$2^2 \cdot 1511$	1263	0.662	9
$L_{8781}^* - 1$	$3 \cdot 2927$	1223	0.582	9
$L_{9072}^* - 1$	$2^4 \cdot 3^4 \cdot 7$	1084	0.385	21
$L_{9356}^* - 1$	$2^2 \cdot 2339$	1955	0.527	18
$L_{10821}^* - 1$	$3 \cdot 3607$	1508	0.407	15
$L_{11221}^* - 1$	$7^2 \cdot 229$	2002	0.342	61
$L_{11808}^* - 1$	$2^5 \cdot 3^2 \cdot 41$	1606	0.361	39
$L_{13173}^* - 1$	$3 \cdot 4391$	1835	0.500	12
$L_{13876}^* - 1$	$2^2 \cdot 3469$	2900	0.384	37

7. RECENT DEVELOPMENTS

After the original version of this paper had been submitted we were pleased to learn from J. Brillhart that he had decided to put together a paper with a collection of identities for primitive parts F_n^* that he had been keeping in his notebooks for many years. This paper [3] particularly contains a general expression for $F_{q^r p^s}^* - 1$ in terms of some other Fibonacci numbers. That expression includes the special formula crucially applied in our Section 4, and some of those given in Section 5 as well.

As we had the privilege of seeing an early draft of Brillhart's enlightening note, we could profitably use his ideas for developing a number of further identities that are provisionally assembled in [9]. They include expressions for $L_n^* - 1$ with subscripts of the form $n = 2^t q^r p^s$, where $t \geq 0$ and $q = 3, 5, 7$.

The following two formulas are special cases corresponding to ones from [3] and [9], respectively, and were applied to verify the new primes F_{14203}^* and L_{11221}^*, now added to Table 2. They also give an idea of certain similarities generally observed in such identities:

$$F_{7p}^* - 1 = 5F_{p-1}F_{p+1}\frac{25F_p^4 - 10F_p^2 + 4}{13},$$

$$L^*_{7^2p} - 1 = 5F_{7(p-1)}F_{7(p+1)}\frac{L^4_{7p} + 848L^2_{7p} + 713182}{599786069}.$$

The entries $L^*_n - 1$ of Table 2 whose subscripts n have three different prime factors (as well as several smaller primes L^*_n of that kind) are also related to explicit formulas given in [9]. Previously the factors needed for a prime-proof in those cases had only been determined experimentally.

8. Factor tables

Many of the factorizations needed for our primality proofs were taken from the tables in [5] and their update [10], which cover Fibonacci numbers F_n for odd $n \le 1000$ and Lucas numbers L_n for all $n \le 500$. However, many factorizations needed beyond these limits were specifically obtained during the course of this investigation. Thus the occurrence of large prime cofactors was often decisive for the completion of a proof.

The means used were essentially the factoring and prime-proving procedures of the UBASIC package [13], R. P. Brent's vectorized ECM implementation [1], and the first author's program for the "$p-1$" method.

Based on a rather modest collection of factorizations of numbers L_n we had gathered for $500 < n \le 1000$, P. Montgomery has added to this a considerable number of more significant factorizations. Currently he is maintaining the extension table [11] covering that segment.

Special mention should be made of two "difficult" factorizations in the extended range that were kindly produced at our request. H. J. J. te Riele, using PPMPQS, split the 90-digit cofactor of L^*_{891} into a p35 · p56 product to enable us to complete the proof for L_{10691}, and Montgomery, using SNFS, split the 118-digit cofactor of L^*_{601} into a p44 · p75 product to enable us to complete the proof for L^*_{10821}.

Regardless of their possible involvement in primality proofs, we have continued doing factoring work for numbers F_n and L_n with $1000 < n \le 9750$. The result is recorded in [8] and includes, in particular, a listing of all primitive prime divisors $p < \max(2^{34}, 4 \cdot 10^6 n)$. They were determined by trial division taking advantage of certain linear dependencies on n that are summarized in Theorems 2 and 3 of [5].

In the Supplement to this paper we assemble all the complete factorizations of numbers F_n (Table I) and L_n (Table II) that we have obtained. The notation used to display the algebraic structure of each number is that of [5]. Both tables include factorizations with probable prime "final" factors whose primality could not yet be established. Note that in this context "complete" does not necessarily mean that all the algebraic factors of a listed number have also been completely factored.

Within the range of the Supplement, the factorizations of L^*_{1181} and L^*_{1347} had previously been obtained by Montgomery, and F^*_{2361} had been proven prime by Morain, in order to be used in the prime-proofs of [12] that were carried out in 1990. Furthermore, the factorizations of F^*_{1015} and F^*_{1035} have recently been completed by Thomas Sosnowski.

9. An extraordinary coincidence

A glimpse at Table I in the Supplement led us to the casual observation that the large primitive parts F^*_{12987} and F^*_{13797}, two clearly different probable prime numbers, have the same number of digits, which is 1626. More amazingly, a closer

look at these primitive parts revealed that they even coincide in their first 26 digits, since

$$F^*_{12987} = 122409585368806223670564423991 9\ldots 92961,$$
$$F^*_{13797} = 122409585368806223670564424561 2\ldots 77761,$$

the second number being "slightly" larger than the first.

The reason for this striking coincidence is an equally surprising similarity in the structure of the subscripts. They are both of the form $n = 3^3uv$, where u, v are primes, and $uv-u-v$ has the same value in both cases. In fact, $12987 = 3^3 \cdot 13 \cdot 37$ and $13797 = 3^3 \cdot 7 \cdot 73$, where $13 \cdot 37 - 13 - 37 = 7 \cdot 73 - 7 - 73 = 431$.

The role played by these relations becomes apparent when an attempt is made to give an estimate of $\log(F^*_n)$ for the special form of n, based on the expression

$$F^*_{3^3uv} = \frac{F_{3^3}F_{3^2u}F_{3^2v}F_{3^3uv}}{F_{3^2}F_{3^3u}F_{3^3v}F_{3^2uv}} = 5777 \cdot \frac{F_{3^2u}F_{3^2v}F_{3^3uv}}{F_{3^3u}F_{3^3v}F_{3^2uv}},$$

where $5777 = F_{3^3}/F_{3^2}$. Since for reasonably large n we have $\log(F_n) \approx n\log(\alpha)$, the logarithm of the last fraction approximately becomes

$$(3^3 - 3^2)(uv - u - v) \cdot \log(\alpha) = 18 \cdot 431 \cdot \log(\alpha) = 7758 \cdot \log(\alpha).$$

Adding $\log(5777)$ to the result and doing all the calculations with high precision, we obtain $\log(F^*_n) = 1625.087815426876\ldots$, whose inverse logarithm exactly reproduces the first 49 digits of F^*_{12987}. These include the complete string of common initial digits of the two numbers F^*_n in question.

We then investigated the possible uniqueness of this phenomenon. Obviously, there are many pairs (n_1, n_2) such that $F^*_{n_1}$ and $F^*_{n_2}$ are "almost equal" in the above sense. We have only to look for pairs (u_1, v_1), (u_2, v_2) of odd primes with $u_1v_1 - u_1 - v_1 = u_2v_2 - u_2 - v_2 = c$. Here the smallest possible constant is $c = 71$, which occurs for $(u, v) = (7, 13)$, $(5, 19)$, giving $(n_1, n_2) = (2457, 2565)$. The next examples are $(n_1, n_2) = (3861, 4185)$, $(5049, 5535)$, $(5481, 5805)$, $(5643, 5859)$, ...

In spite of this rather frequent occurrence, among all couples of pairs (u, v) having $c \leq 623$ the only two of the involved primitive parts that happen to be primes (or probable primes) are the numbers F^*_{12987} and F^*_{13797}. It is just this accidental fact that makes them so exceptional. Incidentally, there is a third pair (u, v) with $c = 431$, leading to another seemingly equal primitive part, which is F^*_{14715}. This one, however, is divisible by the prime $p = 310074481$.

Acknowledgments

We are very grateful to John Brillhart and to Peter Montgomery for their important contributions to this paper, not all of which may be apparent to the reader. Thanks are also due to François Morain for calling our attention to his preprint [12].

References

1. R. P. Brent, *MVFAC: A vectorized Fortran implementation of the elliptic curve method*, Comput. Sci. Lab., Austral. Nat. Univ., 1991.
2. J. Brillhart, electronic mail to W. Keller dated 24 October 1994.
3. ———, *Note on Fibonacci primality testing*, Fibonacci Quart. (to appear).
4. J. Brillhart, D. H. Lehmer, and J. L. Selfridge, *New primality criteria and factorizations of* $2^m \pm 1$, Math. Comp. **29** (1975), 620–647; Errata, Math. Comp. **39** (1982), 747. MR **52:**5546; MR **83j:**10010

5. J. Brillhart, P. L. Montgomery, and R. D. Silverman, *Tables of Fibonacci and Lucas Factorizations*, Math. Comp. **50** (1988), 251–260; *Supplement*, ibid., S1–S15. MR **89h:**11002
6. C. Caldwell, *Review of "The Dubner PC cruncher – A microcomputer coprocessor card for doing integer arithmetic"*, J. Recreational Math. **25** (1993), 56–57.
7. D. Jarden, *Recurring sequences*, 3rd ed., Riveon Lematematika, Jerusalem, 1973; Review of the 2nd ed. (by J. Brillhart) , Math. Comp. **23** (1969), 212–213; Errata, Math. Comp. **25** (1971), 200–201, and Math. Comp. **26** (1972), 1029–1030. MR **20:**4663 (1st ed.); MR **53:**4451; MR **47:**1731
8. W. Keller, *Factors of F_n and L_n for* $1000 < n \leq 9750$, machine-readable table, March 1996.
9. ———, *Some identities for primitive parts of Fibonacci and Lucas numbers*, unpublished notes, July 1996.
10. P. L. Montgomery, *Status of composite Fibonacci and Lucas cofactors*, machine-readable table, August 1996.
11. ———, *Lucas extensions*, machine-readable table, August 1996.
12. F. Morain, *On the primality of F_{4723} and F_{5387}*, preprint, July 1990.
13. W. D. Neumann, *UBASIC: a Public-Domain BASIC for Mathematics*, Notices Amer. Math. Soc. **36** (1989), 557–559; *UBASIC Update*, ibid. **38** (1991), 196–197.

449 Beverly Road, Ridgewood, New Jersey 07450
E-mail address: 70327.1170@compuserve.com

Regionales Rechenzentrum der Universität Hamburg, 20146 Hamburg, Germany
E-mail address: keller@rrz.uni-hamburg.de