MATHEMATICS OF COMPUTATION
VOLUME 50, NUMBER 181
JANUARY 1988, PAGES 251-260

Tables of Fibonacci and Lucas Factorizations

By John Brillhart, Peter L. Montgomery, and Robert D. Silverman

Dedicated to Dov Jarden

Abstract. We list the known prime factors of the Fibonacci numbers F_n for $n \leq 999$ and Lucas numbers L_n for $n \leq 500$. We discuss the various methods used to obtain these factorizations, and primality tests, and give some history of the subject.

1. Introduction. In the Supplements section at the end of this issue we give in two tables the known prime factors of the Fibonacci numbers F_n, $3 \leq n \leq 999, n$ odd, and the Lucas numbers L_n, $2 \leq n \leq 500$. The sequences F_n and L_n are defined recursively by the formulas

$$(1.1) \qquad \begin{aligned} F_{n+2} &= F_{n+1} + F_n, \quad F_0 = 0, \quad F_1 = 1, \\ L_{n+2} &= L_{n+1} + L_n, \quad L_0 = 2, \quad L_1 = 1. \end{aligned}$$

The use of a different subscripting destroys the divisibility properties of these numbers.

We also have the formulas

$$(1.2) \qquad F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}, \qquad L_n = \alpha^n + \beta^n,$$

where $\alpha = (1 + \sqrt{5})/2$ and $\beta = (1 - \sqrt{5})/2$. This paper is concerned with the multiplicative structure of F_n and L_n. It includes both theoretical and numerical results.

2. Multiplicative Structure of F_n and L_n. The identity

$$(2.1) \qquad F_{2n} = F_n L_n$$

follows directly from (1.2). Although the Fibonacci and Lucas numbers are defined additively, this is one of many multiplicative identities relating these sequences. The identities in this paper are derived from the familiar polynomial factorization

$$(2.2) \qquad x^n - y^n = \prod_{d|n} \Phi_d(x, y), \qquad n \geq 1,$$

where $\Phi_d(x, y)$ is the dth cyclotomic polynomial in homogeneous form.

Define the *primitive part* F_d^* of F_d to be

$$(2.3) \qquad F_d^* = \begin{cases} 1, & d = 1, \\ \Phi_d(\alpha, \beta), & d \geq 2. \end{cases}$$

Received February 9, 1987; revised April 27, 1987.

1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11A51, 11B39; Secondary 68-04.

Key words and phrases. Factor tables, Fibonacci, Lucas, factorizations.

Then we have the factorization

$$F_n = \prod_{d|n} F_d^*, \qquad n \geq 1. \tag{2.4}$$

Here the F_d^* are rational integers, computable by the inverse formula

$$F_d^* = \prod_{\delta|d} F_\delta^{\mu(d/\delta)}, \qquad d \geq 1, \tag{2.5}$$

where μ is the Möbius function. The ratio $F'_n = F_n/F_n^*$ is called the *algebraic part* of F_n.

Formula (2.4) reduces factoring F_n to factoring the F_d^*'s. Formula (2.5) shows that the primitive part can be obtained without factoring.

A prime factor of F_n (resp. L_n) is called *primitive* if it does not divide F_k (resp. L_k) for $1 \leq k < n$; otherwise it is called *algebraic.* A composite factor of F_n is also called *algebraic* if it is a product of prime algebraic factors. Any prime divisor of F'_n (resp. L'_n) is necessarily algebraic, but under certain circumstances a prime divisor of F_n^* (resp. L_n^*) is not primitive. Such an algebraic prime factor p of F_n^* (resp. L_n^*) is called *intrinsic* and is listed as p^* in these tables. This occurs exactly when $n = p^r m$, $r \geq 1$, where p is a primitive factor of F_m (resp. L_m). In this case p always divides F_n^* (resp. L_n^*) to just the first power.

Example. The factorization of F_{105}, given by (2.4), is

$$F_{105} = \prod_{d|105} F_d^* = F_1^* F_3^* F_5^* F_7^* F_{15}^* F_{21}^* F_{35}^* F_{105}^*.$$

This factorization is abbreviated in Table 2 as

105 (3, 5, 7, 15, 21, 35) 8288823481.

Here the numbers within the parentheses are the subscripts of the algebraic factors F_d^*, $1 < d < 105$. (The factor $F_1^* = 1$ is omitted.) The primitive part $F_{105}^* =$ 8288823481 is given after the parentheses. The lines in Table 2 corresponding to the numbers inside the parentheses are:

3 $\underline{2}$
5 $\underline{5}$
7 $\underline{13}$
15 (3, 5) $\underline{61}$
21 (3, 7) $\underline{421}$
35 (5, 7) $\underline{141961}$

The factorization of F_{105} is then obtained by collecting the primitive prime factors from their respective lines. These follow the parentheses (if any) on the seven lines and are underlined above for emphasis. Thus,

$$F_{105} = 2 \cdot 5 \cdot 13 \cdot 61 \cdot 421 \cdot 141961 \cdot 8288823481.$$

Because of (2.1), the algebraic multiplicative structure for L_n can be derived directly from that of F_{2n}. Let $n = 2^s m$, where m is odd. Then

$$L_n = \prod_{d|m} L_{2^s d}^*, \qquad n \geq 1, \tag{2.6}$$

where

$$L^*_{2^s d} = F^*_{2^{s+1} d} = \prod_{\delta | d} L^{\mu(d/\delta)}_{2^s \delta}, \qquad d \geq 1. \tag{2.7}$$

The *primitive part* of L_n is $L^*_n = F^*_{2n}$. The *algebraic part* of L_n is

$$L'_n = L_n / L^*_n. \tag{2.8}$$

Furthermore, as a result of a generalization by Lucas of a special identity discovered by Aurifeuille, we also have for odd n

$$\begin{aligned} \frac{L_{5n}}{L_n} &= \frac{\alpha^{5n} + \beta^{5n}}{\alpha^n + \beta^n} = \alpha^{4n} - \alpha^{3n}\beta^n + \alpha^{2n}\beta^{2n} - \alpha^n\beta^{3n} + \beta^{4n} \\ &= (\alpha^{2n} - 3\alpha^n\beta^n + \beta^{2n})^2 + 5\alpha^n\beta^n(\alpha^n - \beta^n)^2 \\ &= (5F_n^2 + 1)^2 - 25F_n^2 \\ &= (5F_n^2 + 5F_n + 1)(5F_n^2 - 5F_n + 1) \text{ (using } \alpha\beta = -1 \text{ and } \alpha - \beta = \sqrt{5}). \end{aligned}$$

Consequently, we have the special Aurifeuillian factorization

$$L_{5n} = L_n A_{5n} B_{5n}, \qquad n \text{ odd}, \tag{2.9}$$

where

$$A_{5n} = 5F_n^2 - 5F_n + 1, \qquad B_{5n} = 5F_n^2 + 5F_n + 1.$$

This decomposition means that these L_{5n}'s have two different algebraic factorizations. For example, from (2.6) and (2.9)

$$L_{105} = \prod_{d|105} L^*_d = L^*_1 L^*_3 L^*_5 L^*_7 L^*_{15} L^*_{21} L^*_{35} L^*_{105}$$

and

$$L_{105} = L_{21} A_{105} B_{105}.$$

Primitive parts A^*_n and B^*_n can also be defined for A_n and B_n. Let $n \geq 1$ be odd and set $n = 5^s m, s \geq 0, 5 \nmid m$. Let $\varepsilon_d = \frac{1}{2}\left(1 + \left(\frac{d}{5}\right)\right)$, where $\left(\frac{d}{5}\right)$ is the Legendre symbol. Let

$$\begin{aligned} A^*_{5n} &= \prod_{d|m} [(A_{5n/d})^{\varepsilon_d} (B_{5n/d})^{1-\varepsilon_d}]^{\mu(d)}, \\ B^*_{5n} &= \prod_{d|m} [(A_{5n/d})^{1-\varepsilon_d} (B_{5n/d})^{\varepsilon_d}]^{\mu(d)}. \end{aligned} \tag{2.10}$$

(Here A^*_{5n} and B^*_{5n} are rational integers such that $(A^*_{5n}, B^*_{5n}) = 1$ and $L^*_{5n} = A^*_{5n} B^*_{5n}$.) Then

$$\begin{aligned} A_{5n} &= \prod_{d|m} (A^*_{5n/d})^{\varepsilon_d} (B^*_{5n/d})^{1-\varepsilon_d}, \\ B_{5n} &= \prod_{d|m} (A^*_{5n/d})^{1-\varepsilon_d} (B^*_{5n/d})^{\varepsilon_d}. \end{aligned} \tag{2.11}$$

Thus, in the above example we have

$$A_{105} = A^*_5 B^*_{15} B^*_{35} A^*_{105}, \qquad B_{105} = B^*_5 A^*_{15} A^*_{35} B^*_{105}.$$

Since $A_5^* = A_{15}^* = 1$, these are omitted in Table 3, while B_5^* is written as L_5^* and B_{15}^* as L_{15}^*.

Those Lucas numbers which do not have an Aurifeuillian factorization appear in the tables in the same format as the Fibonacci factorizations. However, the Aurifeuillian factorizations appear in an expanded format. For example, the above factorization appears as:

$$\begin{aligned}&105\ (3,7,21)\ A \cdot B\\ &A\ (15, 35B)\ 21211\\ &B\ (5, 35A)\ 767131.\end{aligned}$$

The list of numbers immediately after the index 105 indicate that L_{105} has the algebraic factors L_3^*, L_7^*, and L_{21}^*. Furthermore, A_{105}^* has algebraic factors L_{15}^* and B_{35}^*, while B_{105}^* has algebraic factors L_5^* and A_{35}^*. In computing A_n^* and B_n^*, the following result is sometimes useful [9, p. 16]:

THEOREM 1 (CROSSOVER THEOREM). *For odd $k, n \geq 1$ where $(5, k) = 1$ and $\left(\frac{k}{5}\right)$ is the Jacobi symbol,*

$$\text{if } \left(\frac{k}{5}\right) = 1, \quad \text{then } A_{5n} \mid A_{5kn} \text{ and } B_{5n} \mid B_{5kn};$$
$$\text{if } \left(\frac{k}{5}\right) = -1, \quad \text{then } A_{5n} \mid B_{5kn} \text{ and } B_{5n} \mid A_{5kn}.$$

The tables are organized using formulas (2.4) and (2.6). As a result, no prime factor appears explicitly more than once in the tables (except intrinsic factors and the repeated factor 2 of L_3). Where space permits, we list the known factors in their entirety on a single line. We list all prime factors of 25 digits or less, carrying over to a second line, without breaking the factor, when necessary. All other factors are listed as either Pxx or Cxx, indicating respectively a prime or a composite cofactor of xx digits. When a factorization is incomplete, we leave space on the line for new factors to be inserted by hand.

3. Factorization Methods. A variety of methods have been used to effect the factorizations given herein. These include the Pollard $p-1$ and Brent-Pollard Rho methods [13], the analogous $p+1$ method [19], the Continued Fraction (CFRAC) method of Morrison and Brillhart [14], Pomerance's Quadratic Sieve (QS) method [8], along with its extensions and improvements (MP-QS) [17], [18], and Lenstra's Elliptic Curve Method (ECM) [11], [13]. Of course, many of the smaller prime factors are quite old, and were originally found by trial division or the difference of squares method.

Some of the methods utilize the form of the prime divisors given by the following theorems [9, p. 11].

THEOREM 2. *Let n be odd and let p be an odd, primitive prime divisor of F_n. Then*

(i) $p \equiv 1 \bmod 4$.

(ii) *if* $p \equiv \pm 1 \bmod 10$, *then* $p \equiv 1 \bmod 4n$.

(iii) *if* $p \equiv \pm 3 \bmod 10$, *then* $p \equiv 2n - 1 \bmod 4n$.

THEOREM 3. *Let n be positive and let p be an odd, primitive prime divisor of L_n. Then*

(i) *if* $p \equiv \pm 1 \bmod 10$, *then* $p \equiv 1 \bmod 2n$.

(ii) *if* $p \equiv \pm 3 \bmod 10$, *then* $p \equiv -1 \bmod 2n$.

4. Primality Testing. In [9, p. 36], Brillhart gave the following results of primality tests on the Fibonacci and Lucas numbers: F_n, $3 \le n < 1000$, is prime if and only if $n = 3, 4, 5, 7, 11, 13, 17, 23, 29, 43, 47, 83, 131, 137, 359, 431, 433, 449, 509, 569, 571$; L_n, $0 \le n \le 500$, is prime if and only if $n = 0, 2, 4, 5, 7, 8, 11, 13, 16, 17, 19, 31, 37, 41, 47, 53, 61, 71, 79, 113, 313, 353$. More recently, H. C. Williams has discovered that $F_{2971}, L_{503}, L_{613}, L_{617}$ and L_{863} are also prime. Williams also states that F_{4723} and F_{5387} are probable primes [21].

For F_n to be prime, $n \ge 5$, it is necessary, but not sufficient, that n be prime. Similarly, L_n can be prime only when n is prime or a power of 2. There are several identities that can be used for primality proofs if one should find either F_n or L_n or their primitive parts to be probable primes. These identities are useful because in proving N prime, the methods of [5] depend upon auxiliary factorizations of $N \pm 1$. For the Fibonacci numbers we have [9, p. 95]:

$$F_{4k+1} - 1 = F_k L_k L_{2k+1}, \qquad F_{4k+3} - 1 = F_{k+1} L_{k+1} L_{2k+1} \tag{4.1}$$

and

$$F_{4k+1} + 1 = F_{2k+1} L_{2k}, \qquad F_{4k+3} + 1 = F_{2k+1} L_{2k+2}. \tag{4.2}$$

For the Lucas numbers we have

$$L_{4k} - 1 = L_{6k}/L_{2k}, \qquad L_{4k} + 1 = (L_{2k} - 1)(L_{2k} + 1) \tag{4.3}$$

and

$$\begin{aligned} L_{4k+1} - 1 &= 5F_k L_k F_{2k+1}, & L_{4k+3} - 1 &= L_{2k+1} L_{2k+2}, \\ L_{4k+1} + 1 &= L_{2k} L_{2k+1}, & L_{4k+3} + 1 &= 5L_{k+1} F_{k+1} F_{2k+1}. \end{aligned} \tag{4.4}$$

For the Lucas Aurifeuillians we have

$$\begin{aligned} A_{5k} - 1 &= 5F_k(F_k - 1), & B_{5k} - 1 &= 5F_k(F_k + 1), \\ A_{5k} + 1 &= (L_{k-1} - 1)(L_{k+1} - 1), & B_{5k} + 1 &= (L_{k-1} + 1)(L_{k+1} + 1). \end{aligned} \tag{4.5}$$

The use of these formulas is apparent. They break the factorizations of $F_n \pm 1$ and $L_n \pm 1$ into factorizations of smaller F_n's and L_n's and thus facilitate the primality test. There are a number of additional formulas of a similar kind for $F_n^* \pm 1$ and $L_n^* \pm 1$.

All factors and cofactors in Tables 2 and 3 with fewer than 85 digits, and not labelled as Cxx, have been proved prime by Silverman using the methods presented in [5, Section 3] and [20]. These methods depend upon auxiliary factorizations of $p-1$, $p+1$, p^2+1, p^2+p+1, and p^2-p+1. If these cyclotomic polynomials have enough small prime factors, then the methods produce very fast proofs of primality along with a compact certificate which can later be used to verify the proof. Andrew Odlyzko has proved all of the remaining probable prime cofactors to be prime using an implementation of the Cohen-Lenstra algorithm [6].

5. History of Tables. Brillhart found many small factors (up to 10 digits) by a direct search program, using Theorems 2 and 3 to restrict the search range for trial division [1], [2]. He later programmed a difference of squares method with modular exclusion to factor $F_{169}, L_{131}, L_{133}, L_{134}, L_{158}, L_{173}$, and L_{237}.

In 1968 Brillhart used D. H. Lehmer's delay line sieve DLS 127 at U. C. Berkeley [10] to factor $F_{255}, L_{166}, L_{214}, L_{252}$, and L_{258}, again using a difference of squares with modular exclusion. The most remarkable of these factorizations,

$$F^*_{255} = 20778644396941 \cdot 20862774425341,$$

was found in just 40 seconds. Although these two factors are very close, there is no known formula which can account for this factorization.

Between 1970 and 1973, Brillhart and Morrison found a large number of complete factorizations using the continued fraction method, CFRAC, on an IBM 360/91 at UCLA [9], [14].

Starting in 1974, J. L. Selfridge and Marvin C. Wunderlich used an improved version of the UCLA program on an IBM 360/65 at NIU in Dekalb, Illinois to factor many 37-41 digit cofactors. They also implemented the first stage of Pollard's just-discovered $p-1$ method, and found many new factors. Earl Ecklund and Brillhart programmed and used the first stage of the $p+1$ method as well [5, p. xlii].

H. C. Williams [19] applied the $p \pm 1$ methods to 174 composite Fibonacci and Lucas cofactors which had at most 80 digits.

Thorkil Naur ran the $p-1$ and Pollard Rho methods on F_n for odd n, $1 \le n \le 399$, and on L_n for $0 \le n \le 500$. When a factor was at most 53 digits, he completed it via CFRAC. His book [15] and paper [16] list several new factorizations which are included herein.

Montgomery, between 1983 and 1986, applied the methods of [13] to all composite table entries, using idle time on a VAX/780, two VAX/750's and a CDC 7600. He found about 200 previously unknown factors of 11 to 36 digits. Over half of these were found by ECM. He used 10 elliptic curves with limits of 10^4 and $6 \cdot 10^5$, another ten curves with limits of $1.6 \cdot 10^4$ and 10^6, and a third set of ten curves with limits of $3.2 \cdot 10^4$ and $2 \cdot 10^6$. Often he used four, five or more sets, but the work is uneven (many more curves were used on the Lucas numbers than on the Fibonacci numbers). Montgomery [13, Section 6] also ran $p+1$ with an initial value (seed) of $15/8 \bmod N$ using limits of $3 \cdot 10^5$ and 10^7, and again with a seed of $23/11 \bmod N$ using limits of $2 \cdot 10^6$ and 10^8. If $P \equiv 15/8 \bmod N$, then $P^2 - 4 \equiv -31/64 \bmod N$ will be a quadratic residue precisely when -31 is a quadratic residue, so this will find a factor of p if $p - \left(\frac{-31}{p}\right)$ is highly composite; this includes cases where 31 divides whichever of $p \pm 1$ is highly composite. The seed of $23/11 \bmod N$ catches cases where $p - \left(\frac{5}{p}\right)$ is highly composite. By Theorems 2 and 3, if $p \mid F^*_n$ (n odd) or $p \mid L^*_n$, then $p - \left(\frac{5}{p}\right)$ is divisible by $2n$, so the latter case occurs frequently. However, these runs did miss some primes p for which $p+1$ is highly composite, such as the factor

$$2170208701449020077201 = 2 \cdot 7 \cdot 12583 \cdot 55807 \cdot 424267 \cdot 520309 - 1$$

of F_{795} (found by MP-QS; -31 is a nonresidue, but the limits were not high enough on that run).

Davis and Holdridge [7], in 1984, completed the factorizations of four cofactors ($F_{277}, L_{362}, L_{370}$, and L_{471}) of 57 to 58 digits, using QS on a CRAY 1S.

Silverman, between 1983 and 1986, ran $p-1$ with limits of $3 \cdot 10^6$ and $5 \cdot 10^7$ on the entire Lucas table and on the Fibonacci table to F_{499}. He also ran $p-1$ with limits of $2 \cdot 10^5$ and $3 \cdot 10^6$ on the Fibonacci table from F_{501} to F_{999}. This work was accomplished on a Micro-VAX/1 and found about 80 new factors. Some runs with ECM on the Lucas table using the same machine revealed no new factors. Silverman also completed the factorizations of all cofactors below 73 digits, and several larger ones, using either CFRAC or MP-QS [17], [18] on a combination of VAX/780's and SUN-3/75's. The larger factorizations were accomplished using a parallel implementation of MP-QS on a network of SUN's.

6. Accuracy and Completeness of Tables. Montgomery and Silverman independently verified each entry in the main tables. They checked that

- Each listed factor divides the number and is a prime or probable prime.
- The proper list of algebraic (including intrinsic) factors appears
- The primitive prime factors appear in ascending order.
- If no cofactor is given, the list of factors is complete.
- If a cofactor is labelled as Cxx, then it is indeed composite and has xx digits.
- If a cofactor is labelled as Pxx, then it is a prime or probable prime and has xx digits.
- No odd primitive prime factor of F_n or L_n was found to divide twice, further strengthening the conjecture that no such prime exists.

Earlier versions of these tables were checked on computers by Michael Morrison and Tim Korb.

As of August 1987 there remain 140 composite Fibonacci cofactors and 10 composite Lucas cofactors in the tables. During 1986 Silverman and Montgomery found numerous factors greater than 20 digits, but none smaller. Based upon numerous runs with ECM, the authors are confident that there are at most 3 undetected factors less than 20 digits.

7. Discussion of Methods. It is still an open question what the best method is to attack a large arbitrary composite number. The authors' experience suggests that the following procedure is perhaps the most reasonable.

As long as the remaining cofactor N is not a probable prime, do the following in order:

(1) Trial division up to some small limit, perhaps $(\ln N)^2$.

(2) ECM is generally more effective than $p \pm 1$, but $p \pm 1$ is so much faster that trying it first is worthwhile. A good first set of starting limits is about 10^4 and 10^5. This should perhaps take a couple of minutes on a typical mainframe for (say) an 80-digit number.

(3) ECM should now be tried, using about 5 curves and limits of 10^4 and $5 \cdot 10^5$.

(4) If the remaining cofactor is sufficiently small (say up to 60 digits), it should be finished with MP-QS. If the number is larger than this, it is worthwhile devoting more ECM trials with higher limits to it.

(5) If ECM fails and the number is less than about 70 digits, then MP-QS should now be applied. Seventy digits will take about a day on a typical modern mainframe. One can of course attempt larger numbers with a supercomputer or special hardware. The largest number ever factored with MP-QS, as of December 1986, was an 87-digit cofactor of $5^{128}+1$ using a parallel implementation on a SUN network. That factorization took 3950 total CPU hours, divided among 10 SUN-3's over a period of about 5 weeks.

(6) Finally, if the cofactor is still too large, one can keep trying ECM with higher limits or set the number aside.

TABLE 1

Prime Factors With More Than 25 *Digits*

N	Factor	Discoverer	Method	Machine
L_{386}	10245029712795120034405043	Montgomery	ECM	CDC 7600
F_{563}	12158771296959377863294133	Montgomery	ECM	CDC 7600
L_{431}	13780495531127210356018421	Silverman	$p-1$	UVAX/1
F_{425}	14187954345303564388390001	Silverman	MP-QS	VAX/780
F_{507}	17340889195212892399797173	Silverman	MP-QS	VAX/8600
L_{406}	23670698911880865758980387	Silverman	MP-QS	VAX/780
L_{371}	35668796989484800666122809	Silverman	MP-QS	VAX/780
L_{422}	36302689192832119042589867	Silverman	MP-QS	SUN-3/75
L_{467}	47381053174782191395897031	Montgomery	ECM	CDC 7600
L_{320}	62379555831803099867272961	Naur	CFRAC	Mathilda
F_{837}	136299772702544437679660333	Silverman	MP-QS	SUN-3/75
F_{445}	156525289282548414081799081	Silverman	MP-QS	VAX/780
L_{471}	478330258123360554199869169	Davis	QS	CRAY 1S
F_{277}	505471005740691524853293621	Davis	QS	CRAY 1S
F_{517}	641466124349607697016238097	Silverman	MP-QS	SUN-3/75
F_{741}	669652072271051271698436113	Silverman	MP-QS	SUN-3/75
F_{597}	1226244816494972899766403949	Silverman	MP-QS	SUN-3/75
F_{503}	2430014747700999423017017501	Silverman	MP-QS	SUN-3/75
F_{869}	5890430821204665088535469913	Montgomery	ECM	CDC 7600
L_{479}	16372649304949588683920725489	Silverman	MP-QS	VAX/780
F_{559}	26093837057017247269531221521	Silverman	MP-QS	SUN-3/75
F_{317}	50354633016533380504238521909	Silverman	MP-QS	VAX/780
F_{461}	57907365333787128886141126177	Silverman	MP-QS	SUN-3/75
F_{633}	192347474285460831200493920089	Silverman	MP-QS	SUN-3/75
L_{326}	573005680996120855900783871963	Silverman	MP-QS	SUN-3/75
F_{971}	619802607259514583330235693729	Montgomery	$p-(5/p)$	CDC 7600
L_{412}	1090414335383168463561145167623	Montgomery	ECM	CDC 7600
L_{344}	1403981099723321029379913948641	Silverman	MP-QS	VAX/780
L_{482}	5373430329122468821883671012169	Montgomery	ECM	CDC 7600
L_{377}	9220407243723719942154317888399	Silverman	MP-QS	SUN-3/75
F_{489}	55010483350408487052485570744297	Silverman	MP-QS	SUN-3/75
F_{663}	542202788462733966380018208818089	Silverman	MP-QS	SUN-3/75
F_{681}	1316534463290847218590097513564513	Silverman	MP-QS	SUN-3/75
L_{430}	1517416544639719175645264380247161	Silverman	MP-QS	SUN-3/75
F_{383}	15318508443810774614619603643486769	Silverman	MP-QS	SUN-3/75
F_{427}	24949586896499848287125235667356281	Silverman	MP-QS	SUN-3/75
L_{464}	227693725298545340302283668318476481	Montgomery	ECM	CDC 7600

The present practical limit of technology seems to be about 16 digits for prime factors found by Pollard Rho, 18 digits for Brent's variation of Pollard Rho, and 25 digits for ECM. The $p \pm 1$ methods occasionally have huge successes where a factor over 25 digits is found; for example, these methods could have found the 29-digit factor of L_{479} with a little more effort. However, factors of 18 to 20 digits are more typical. The CFRAC method has been demonstrated for products up to 10^{64}, QS for products up to 10^{71}, and MP-QS for products up to 10^{87}. This comparison is not quite fair, however, because the CFRAC and QS results were achieved either on a supercomputer or on special purpose hardware, while the MP-QS results were achieved on a network of SUN's [17], [18].

Table 1 lists all of the known nonlargest primitive prime factors of F_n or L_n having more than 25 digits. The cofactor of each of these, when it is composite, is assumed to have at least one prime factor exceeding the factor listed. Each entry includes the discoverer, the method of discovery, and the machine used. In the "machine" column the notation "UVAX/1" is an abbreviation for Micro-VAX/1.

Acknowledgments. The authors wish to thank their institutions for providing the extensive computer time required for this work. Silverman extends special thanks to Tom Caron for writing the networking software that made the parallel implementation of MP-QS possible. Montgomery extends special thanks to Mike Mitchell and Richard Milton for the many hours they spent running his CDC 7600 jobs. All of us extend special thanks to Andrew Odlyzko for providing many of our primality tests and to Dave Cantor, Tim Korb, D.H. and Emma Lehmer, Michael Morrison, J. L. Selfridge, Peter Weinberger, Hugh C. Williams, and Marvin C. Wunderlich for their assistance over the years in helping to create these tables.

Department of Mathematics
University of Arizona
Tucson, Arizona 85721

UNISYS
2525 Colorado Avenue
Santa Monica, California 90406

MITRE Corporation
Burlington Road
Bedford, Massachusetts 01730

1. J. BRILLHART, "Fibonacci century mark reached," *Fibonacci Quart.*, v. 1, 1963, p. 45.

2. J. BRILLHART, "Some miscellaneous factorizations," *Math. Comp.*, v. 17, 1963, pp. 447–450.

3. J. BRILLHART, D. H. LEHMER & J. L. SELFRIDGE, "New primality criteria and factorizations of $2^m \pm 1$," *Math. Comp.*, v. 29, 1975, pp. 620–647.

4. J. BRILLHART, "UMT of F_n for $n \leq 3500$ and L_n for $n \leq 1750$," *Math. Comp.*, submitted to unpublished tables.

5. J. BRILLHART, D. H. LEHMER, J. L. SELFRIDGE, B. TUCKERMAN & S. S. WAGSTAFF, JR., *Factorizations of* $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *Up to High Powers*, Contemp. Math., vol. 22, Amer. Math. Soc., Providence, R.I., 1983.

6. H. COHEN & H. W. LENSTRA, JR., "Primality testing and Jacobi sums," *Math. Comp.*, v. 42, 1984, pp. 297–330.

7. J. A. DAVIS & D. B. HOLDRIDGE, *Most Wanted Factorizations Using the Quadratic Sieve*, Sandia Report SAND84-1658, 1984.

8. J. L. GERVER, "Factoring large numbers with a quadratic sieve," *Math. Comp.*, v. 41, 1983, pp. 287–294.

9. D. JARDEN, *Recurring Sequences*, 3rd ed., Riveon Lematematika, Jerusalem, 1973.

10. D. H. LEHMER, "An announcement concerning the Delay Line Sieve DLS 127," *Math. Comp.*, v. 20, 1966, pp. 645–646.

11. H. W. LENSTRA, JR., "Factoring integers with elliptic curves," Ann. of Math. (To appear.)

12. PETER L. MONTGOMERY, "Modular multiplication without trial division," *Math. Comp.*, v. 44, 1985, pp. 519–521.

13. PETER L. MONTGOMERY, "Speeding the Pollard and elliptic curve methods of factorization," *Math. Comp.*, v. 48, 1987, pp. 243–264.

14. M. A. MORRISON & J. BRILLHART, "A method of factoring and the factorization of F_7," *Math. Comp.*, v. 29, 1975, pp. 183–205.

15. T. NAUR, *Integer Factorization*, DAIMI PB-144, Computer Science Department, Aarhus University, Denmark, 1982.

16. T. NAUR, "New integer factorizations," *Math. Comp.*, v. 41, 1983, pp. 687–695.

17. ROBERT D. SILVERMAN, "The multiple polynomial quadratic sieve," *Math. Comp.*, v. 48, 1987, pp. 329–339.

18. ROBERT D. SILVERMAN, "Parallel implementation of the quadratic sieve," *The Journal of Supercomputing*, v. 1, 1987, no. 3.

19. H. C. WILLIAMS, " A $p+1$ method of factoring," *Math. Comp.*, v. 39, 1982, pp. 225–234.

20. H. C. WILLIAMS & J. S. JUDD, "Some algorithms for prime testing using generalized Lehmer functions," *Math. Comp.*, v. 30, 1976, pp. 867–886.

21. H. C. WILLIAMS, private communication.