III. Introduction to the Main Tables*.

> "The invention of new [factorization] methods may push off the limits of the unknown a little farther, just as the invention of a new astronomical instrument may push off a little the boundaries of the physical universe; but the unknown regions are infinite, and if we could come back a thousand years from now, we should no doubt find workers in the theory of numbers announcing in the journals new schemes and new processes for the resolution of a given number into its factors."
>
> *D. N. Lehmer* [**66**]

A. The Cunningham-Woodall Tables and Their Influence— The Cunningham Project

In 1925, Lt.-Col. Allan J. C. Cunningham and H. J. Woodall published a small volume of tables [**11**] of factorizations of $b^n \pm 1$ for the bases $b = 2$, 3, 5, 6, 7, 10, 11, 12 to various high powers n. These tables collected from scattered sources the known prime factors for the bases 2 and 10 and also presented the authors' results of thirty years' work with these and the other bases. (See [**11**, pp. xii, xviii] and [**55**] for a general survey of factor tables.)

For decades these useful tables served as a basic reference on factors of these numbers. The tables were not only a summary of what was known, but a disclosure of what was not. Furthermore, by leaving blanks in the tables where new factors could be entered, by putting question marks on numbers of unknown character, and by giving credit to those who had discovered notable prime factors in the past, the authors stimulated work on the remaining composite numbers in the tables.

In the *Introduction* to the tables, a somewhat unsatisfactory account of the multiplicative structure of $b^n \pm 1$ was given in a rather finicky notation and terminology. Many useful examples were given to illustrate how numbers of the different forms factor. However, much remained unsaid as to just how the numbers factor algebraically and how the various algebraic factors divide one another.

This is particularly true in the section on Aurifeuillian factorization, where there is no mention of the form of the primitive part in such factorizations. As is clear from the parenthetic remark at the bottom of page vi, the authors knew neither this form nor the rule that determines which L or M will divide another L or M [**36**, p. 181]. All in all, though, this pleasant and important little book—a labor of love—was and is much valued by those who are fortunate enough to own a copy.

In the fifty years following 1925, some copies of these tables became so filled with inserted factors and other information that the present volume, which we consider to be an extension and an updating of the earlier tables, comes none too soon. Many new prime factors have been discovered in the last thirty years through the use of computers and by new methods of factoring and primality testing. Evidence of this abundance can be seen, for example, in the fact that all the numbers in the

*The text of this Introduction is essentially that used in the first edition. A few typographical errors were corrected and the old status report was deleted. The new text for the second edition appears in Section **IV**. The new text for the third edition appears in Section **V**.

Cunningham-Woodall base three tables (up to $n = 111$) are completely factored in the present work, and that it is no longer feasible to keep track of the discoverers of all the new prime factors.

In a way, it is sad that rapid and accurate automatic computers have spoiled the hand calculator's pleasure and feeling of accomplishment in factoring what was an immense number. Indeed, many of the factors in these tables were monuments in their day to this kind of achievement. But transcending the limits of human power by machines can bring with it, all the same, a new sense of power in achievement and also a freedom from drudgery which may well stimulate the devising of new methods and the setting of new goals when the old goals are reached. And certainly, there is still a real feeling of accomplishment in breaking apart some huge number which has withstood assaults for decades, especially when in doing so one has had to devise and carefully carry out some new computational scheme. The current invasion of small electronic computers into homes and offices may well lead to renewed interest in attacking the large composite numbers still remaining in these tables.

For many years we have referred to the ongoing work on these tables as "The Cunningham Project". As new factors have been found or primality tests have been completed, the accumulation of information has prompted a continual reorganization of the data into forms better suited to updating. The new data, which at first were written in the Cunningham-Woodall tables, were later transferred to boxes of Hollerith cards, making the modification and listing of the tables much simpler. In 1968 BT (authors' initials will be used throughout this work), using an IBM 360/67 at the Thomas J. Watson IBM Research Laboratories, systematically found all factors $< 10^8$ of most of the entries in the present tables (except for base 2), of which many were new. He also discovered the compositeness or probable-primality of all the cofactors using Fermat's congruence, at the suggestion of JLS. This information was incorporated manually into the files of Hollerith cards. In 1970, Mike Morrison and JB subjected the resulting tables to a computer checking scan on the IBM 360/91 at UCLA. Several errors were discovered among the data manually accumulated over the years. In later years, the data were placed in a data set (disk file) on the computer system at Northern Illinois University, DeKalb, along with all the primality testing information that had accumulated for years in an impressive stack of computer printout.

With all the information in a data set (and the large stack of printout happily thrown away), new formats were devised which provided for a simple presentation of prime and algebraic factors in the tables in which a prime factor is listed as such only once at its first appearance. Some of the remaining problems in the tables were identified and listed, and the factoring and primality testing programs available at DeKalb were set to work in an attempt to solve these problems.

Substantial progress has been made over the last several years, and the range of n has been extended in each table, although we have used only the original bases of the Cunningham-Woodall tables.

The present tables are now at the limits of what can be done by factoring through 50 digits using the method in [**75**], although more progress will no doubt be made when the two excellent factoring methods of J. M. Pollard [**80, 81**] have been used more. We have listed in Appendix C the remaining composite cofactors with 64 or fewer digits as an aid or a challenge to venturesome readers. (See **IV** for the progress made between the first and second editions of this book.)

When the tables were essentially ready for distribution, SSW wrote and ran a checking program which tested the factorizations in the different tables to see if: (1) a listed factor actually divided the respective number; (2) all factors were present in complete factorizations; (3) all factors listed were probable primes base 13; (4) the line numbers listed in parentheses were complete and correct. Minor checking was also done to see if the lengths of cofactors were correct and if periods and parentheses were in the right places. Finally, the cofactors themselves were again checked as probable primes base 13 and were stored in the proper appendices along with their labels and lengths.

B. Developments Contributing to the Present Tables.

Since 1925, tremendous developments in technology, factorization and primality testing have contributed to the enlargement and improvement of the Cunningham-Woodall tables. In the account which follows, we have tried to give both a technical and a personal review of events that have been an engrossing and, at times, an exciting part of our lives for many years. Although this account is in no way a history of the developments in these various fields, we do seek to present, as they were seen by us, those aspects which relate to the Cunningham Project.

We have tried to mention those who have contributed in some significant way to these events. It is perhaps worth remarking that few people have ever busied themselves with actually factoring $b^n - 1$ or with testing numbers for primality. We regret this and hope this volume will stimulate others to add to our knowledge of these things.

1. Developments in Technology.

The main technological developments that helped to bring the factor tables into their present form are listed below in roughly chronological order.

(a) *Automatic Multiply and Divide.* In about 1925 automatic multiply and divide operations became available on mechanical calculators in the United States. This improvement reduced errors and computing time, enough so that hand calculation in factorization and primality testing could persist until rather recently. Now, however, even the more accessible calculations are usually done by electronic computers.

Some who worked by hand on problems relating to $b^n - 1$ after 1925 were D. N. Lehmer, DHL and Emma Lehmer [**40**], M. Kraitchik [**34, 35**], P. Poulet [**83** and see **56**], H. S. Uhler [**105, 106**], A. Ferrier [**14** to **19**], N. G. W. H. Beeger [**1**], R. E. Powers [**84**], E. Gabard [**6, 20, 31**], and K. R. Isemonger [**3, 6, 29, 30, 31**]. Their results, usually obtained after long hours of work at a desk calculator, are a tribute to diligent and careful computation.

(b) *The Bicycle-chain Sieve* [**42, 64**]. This machine was built by DHL in 1927 and was the first fully automatic machine to be used for factoring and primality testing. (Prior to this, paper strip methods had been used for hand-sifting [**33**, Ch. 2], as well as various stencil devices such as the factor stencils of D. N. Lehmer [**67, 69, 40**, p. 336] and the Hollerith card stencils of J. D. Elder [**13**].) The scanning rate of the machine was 50 numbers per second, and it produced impressive results for its day, such as the two factorizations

$$10^{20} + 1 = 73.137.1676321.5964848081$$
$$2019210335106439 = 25709599.78539161$$

these latter being factors of $3^{111} + 1$.

(c) *The Photoelectric Number Sieve* [**10, 48, 49, 50, 64**]. This machine was built in 1932 by DHL and his associates. It used electronics that were advanced for its time, as well as high-precision gears to carry out the sifting. Among its many results are the two factorizations

$$2^{79} - 1 = 2687.202029703.1113491139767$$
$$2^{93} + 1 = 3^2.529510939.715827883.2903110321$$

and a proof that the cofactor 3011347479614249131 of $2^{95} + 1$ is a prime. The scanning rate of this machine was 5000 numbers per second. For a delightful account by D. N. Lehmer of the photoelectric number sieve, see [**68**]. (See the status report in section **V B** for more about this machine.)

(d) *The ENIAC (Electronic Numerical Integrator and Computer).* In [**57**] and [**62**] DHL gave an account of how "during a holiday weekend" this machine produced 85 new factors of $2^k \pm 1$ for $k \leq 500$. (See [**56, 63**].) Collecting the results was pleasantly overwhelming—"picking plums at waist height"—considering that a few new factors would be all that the most industrious hand computer would expect to find in months of labor. Here, then, was already an example of a practice that was to be repeated over and over again in the decades to follow: letting a computer factor and test for primality on *idle time*. Many results in these tables were obtained on idle time, quite often to the benefit of the machines which were better left running than being shut down. (In at least two instances these machine-language programs, which the machine operators and IBM engineers came to regard as *test programs*, detected intermittent hardware failures which had evaded the standard machine tests.) The vast amount of time spent organizing the extensive output and the cases to be run, and preparing setups to be run (often throughout the night) attests to the great interest and pleasure we felt at a time when factoring and primality testing had not yet been recognized as being relevant to the transfer of funds or to national security. This persistent involvement over the years has led to a considerable development in the theory and the practice of factoring and primality testing.

(e) *The SWAC (Standards Western Automatic Computer).* This was the first large electronic computer in the western United States (UCLA, 1950). Although this machine had a memory of only 256 words of 37 bits each (later augmented with a 4096-word drum), it was a very nice binary machine which allowed for flexible bit manipulation with its four-address system. It had a 16 microsecond cycle time, a bit-parallel addition taking 4 cycles and a multiplication taking 23. It was directly suitable for number theory in that it, unlike some more modern general purpose computers, produced an exact double-word integer product.

Much number theory was done on this machine [**70**]. At least three programs run on the SWAC dealt with material in this book. One was a Fermat number factoring routine written by JLS [**95**] which discovered factors of $2^{2^{10}}+1$ and $2^{2^{16}}+1$ in 1953. The other two were written by Raphael M. Robinson, who caused a mild sensation by programming a primality test for the Mersenne numbers $M_p = 2^p - 1$ which ran when first tried, even though he had never programmed a computer before. His modest account is given in [**90**]: "The program was first tried on the SWAC on January 30 [1952], and two new [Mersenne] primes were found *that* *day* (our emphasis), three other primes were found on June 25, October 7, and October 9" [and see MTAC **6** (1952) 61, 205; **7** (1953) 72]. These were the primes corresponding to $p = 521, 607, 1279, 2203$ and 2281. In addition to discovering this impressive list of new Mersenne primes, the program was used to check the Mersenne number results found earlier by hand calculation.

The second program of Robinson was used by Robinson and JLS to find factors of the Fermat numbers $F_n = 2^{2^n} + 1$. Although the machine was somewhat unreliable because of its Williams tube electrostatic memory, it was a wonderful machine with which to reach out beyond human powers. One minute of SWAC time was roughly equivalent to one year of desk calculator time.

When programmed as a sieve, the SWAC was capable of sifting 100,000 numbers a minute, only one-third the speed that the photoelectric number sieve had achieved twenty years earlier.

A charming feature of the SWAC was its loudspeaker which emitted squawks and noises characteristic of the loops in the running program. After running the program for a while, the machine operator, who was usually the programmer, could tell more or less what the computer was doing by just listening to it.

(f) *The IBM 701.* One of these machines was installed at UC Berkeley in 1954 and was taken out in 1962. Originally it had an electrostatic Williams tube memory like the SWAC, but in a short time it was given a magnetic core memory and so became much more reliable.

Many researchers owe a great deal to Ted Ross, the IBM engineer who made the 701 the reliable machine that it was for its full life at Berkeley. The computer had a reasonably large memory and a peripheral magnetic drum for slower extra storage. Its cycle time was 12 microseconds. An addition took 5 cycles, a multiplication or division 38. It was a fine machine for number theory, since it gave a double-word product and an exact quotient and remainder on division. It also had a good set of "bit-pushing" instructions which facilitated some ingenious machine-language programming.

The computer could operate at either a full or a half-word level, each word consisting of 35 bits and a sign. The arithmetic on the machine was in signed binary, in contrast to the now common twos-complement arithmetic which can be awkward.

Within a few years of operation, the 701's library of programs had some very useful software, such as a good symbolic assembler and several types of dumps, including a snap dump and a couple of trace dumps. There were three magnetic tape units that gave the system greater flexibility in operation. On the other hand, there was no higher level language and the hardware itself was lacking in many ways. There was no BCD, no floating-point arithmetic, and there were no index registers. It was also necessary to program all input-output and all the checking that went with it. All programs were initially loaded on-line through the card reader.

Three different projects contributing to these tables were carried out on the 701. In [**92**] Raphael M. Robinson reported on a direct search for factors using a difference table to generate the sequence of trial divisors. From this search came several complete factorizations as well as the first factors of the Mersenne numbers M_{109} and M_{157}.

In [**2**], six new factors of $2^p - 1$ for $p = 163$, 181, 193, 229, 239 and 241 were reported, along with many other factors of M_p obtained by direct search. Because this search was done at zero priority, a considerable effort was made to minimize the search time by using a succession of divide routines requiring fewer machine cycles for larger divisors. Whenever the divisor surpassed a certain power of two, a new program was manually loaded. In [**3**], another direct search produced many new factors of the numbers $2^{2p} + 1$, p prime. This program also keyed the divide routines to the growing size of the divisors, but this time the program itself kept track of their size and wrote the routine to be used on the next larger class of divisors.

DHL also wrote a primality test for numbers $2^p \pm 2^{(p+1)/2} + 1$ which had no known prime factors. In this way, for instance, $2^{379} + 2^{190} + 1$ was discovered to be a prime. The factoring program completely factored two numbers, namely $2^{83} - 2^{42} + 1$ and $2^{59} + 2^{30} + 1$, the latter having been listed as a prime in 1929 by Kraitchik [**35**, p. 87].

(g) *The IBM 704.* This machine was a tremendous improvement over the 701, with which it was incompatible. It was the first of the series of IBM computers—numbered 704, 709, 7090, 7094—that, like the 701, were excellent for number theory. Internally they used signed binary arithmetic.

The hardware improvements in the 704 were many. It had, for example, three index registers, a larger instruction repertoire, BCD mode, floating-point arithmetic, automatic input-output checking, simpler-to-use magnetic tape drives, and a more rapid card reader. The assembler was also much improved. As with all the IBM computers, the 704 was excellently maintained and was very reliable.

A number-theoretic subroutine package for multiple-precision arithmetic was written in machine-language for this machine by Jerry (G. D.) Johnson, and the package turned out to be compatible with all the later machines in this series. This package permitted left and right shifting of binary words and contained the basic number-theoretic subroutines for signed integers that allowed for their addition, subtraction, multiplication and division, and also the computation of $a^n \pmod{m}$, the GCD, and the Jacobi symbol.

Several programs based on this package of subroutines were written by JB and were much used on this project. Among these were a direct-search factoring program as well as a primality testing program which could determine the primality of a probable prime N when the complete factorization of $N - 1$ was known.

The main results obtained on this machine were the discovery of a second factor of F_{10} and the factorization of

$$M_{101} = 7432339208719.341117531003194129\,.$$

The latter was obtained in 1963 by Jerry Johnson, DHL and JB from a direct search based on a quadratic sieve constructed from quadratic residues in the continued fraction expansion of $\sqrt{mN}$ for various values of m. To produce these residues, the 704 ran for hundreds of hours without an error! M_{101} had been the smallest composite Mersenne number with no known factors, and this factorization had been sought for decades. It was discovered in only two hours because the sequence of trial divisors had such large differences between consecutive terms.

(h) *The Delay-line Sieves (DLS 127, DLS 157)* [**59, 64, 7**]. In December of 1965 the delay-line sieve DLS 127 ("Dick Lehmer's Sieve") [**6**] began running at UC

Berkeley. This sieve, which was designed by DHL and made operational through the good offices and efforts of Paul Morton and Robert Coffin, used electronic delay-lines in place of the earlier bicycle chains and gears. Its scanning rate, as well as that of the later DLS 157, was 10^6 numbers per second. The later model, DLS 157, which is still running, was made from DLS 127 by adding shift registers (instead of more delay-lines) for the prime moduli from 131 to 157. Both sieves operated on 100 watts of power. (See the status report in section **IV B**.)

An interesting design problem that had to be solved in building the sieve was how to save the bit patterns in the delay-lines during their individual sieving when it was necessary to pause long enough to print out a solution that the sieve had just discovered. To do this, the individual bit patterns were hooked end to end and circulated as a serpentine through the whole machine. Whenever the serpentine had returned to its original position, the individual sieving could then be started again [**64**].

Many factorizations and primality tests were done using these sieves. The notable factorization,

$$2^{109} - 2^{55} + 1 = 5.74323515777853.1746518852140345553$$

was completed on the DLS 127 by a difference of squares method. These sieves are the most rapid we have used, the nearest competitor being a sieve program with a scanning rate of about 10^5 numbers per second, written by JB [**6**] for the IBM 7094.

(i) *The IBM 709, 7090, 7094.* These machines continued the trend begun by the 704, the tubes in the 709 being replaced by transistors in the latter two machines. The 7094 had 7 index registers, and a marvelous and useful array of machine instructions. The cycle time was 2.18 microseconds, with add, multiply and divide times of 2, 5 and 8 cycles, respectively.

Careful programming of the data channels on the machine permitted input and output that were independent of the main processor and parallel to it. There was also an excellent collection of standard programs for assemblies, dumps, trace routines, and other debugging aids.

The machines used were primarily those at UC Berkeley, Stanford (thanks to G. Forsythe) and UCLA. In the latter part of its life, the 7094, which was owned by UC Berkeley, sat in the basement of the mathematics building. It had no data channels or maintenance contracts, for it had been superseded by the CDC 6400. Nonetheless, since factoring programs require little input and produce little output, the 7094 gave JB, JLS, DHL and Emma Lehmer a marvelous opportunity to work. Thus with patience we put the program into the memory in binary through the console switches. Of course no one else was using the machine, so it became essentially our machine. When after months of excellent service some hardware began to fail, we either programmed around the difficulty or dug into our pockets for a little money to bring in an IBM engineer to fix the machine.

In the days before its final sad demise, JB wrote some factoring and primality testing programs based on the multiple-precision package of Jerry Johnson. The primality program tested the primality of a probable prime N, given the complete factorization of $N - 1$. Later, a more elaborate program was written by JB which automated the passing between levels in primality testing [**4**]. This program was a predecessor of the DOWNRUN program of JLS and Marvin Wunderlich, used extensively at DeKalb and described in **3**(b) below.

JB wrote not only a simple direct search factoring program, but also a very productive difference of squares program [**6**]. Results obtained by the latter program include the factorizations of M_{103}, M_{163} and

$$2^{107} + 2^{54} + 1 = 843589.8174912477117.23528569104401 .$$

A large number of factorizations obtained on the 7090 and the 7094 appear in these tables for the first time, but are lost in the profusion of more recent results.

Some primality testing on Fermat and Mersenne numbers was done by JLS and Alex Hurwitz at UCLA [**96**]. They ran a modular check during the testing on each arithmetic operation and discovered over a long period of time that the machine did in fact make several arithmetic errors. Of course, such primality testing made unusually heavy repetitive use of the fixed point instructions. BT developed a package of Fortran and Assembly language multiple-precision integer arithmetic and trial-divisor factorization programs for the 7094 at the IBM Research Center, and used it for work on odd perfect numbers in 1967 [**103, 104**]. This work depended on the evaluation and factorization of a number of values of $\sigma(n)$, the sum-of-divisors function. As is well known, if $n = \prod_i p_i^{a_i}$, then $\sigma(n) = \prod_i \sigma(p_i^{a_i})$ and $\sigma(p^a) = (p^{a+1} - 1)/(p - 1)$. Aside from the denominator $p - 1$, this is of the same form as the numbers $b^n - 1$ considered in the present work, where $b = p$, $n = a + 1$. However, the interest extended to a greater range of prime values p of the base, and a lesser range of the exponent, than the present work. Complete factorizations were made of all cyclotomic numbers $\Phi_q(p) < 10^{18}$ for which p and q are odd primes, and $p > 14$, also for scattered larger p as needed, some also for $q = 2$. These factorizations may be found in [**104**]. The ones for $p < 12$ are subsumed in the present tables.

Perhaps the most impressive computer center that we used was at the Bell Telephone center at Holmdel, New Jersey. Several 7094's were hooked into a single system. They could be switched for different use as easily as one could reassign the numbers on a tape unit. This center came close to the ideal of having a system which was not so generalized that simple, standard things couldn't be done simply. Among the single user machines the 7094 was indeed outstanding for number theory.

(j) *The IBM 360 Series.* With the introduction of this series of computers, the single-user became one of the several persons using the machine at the same time. The word size was shrunk to 32 bits, and the machine was incompatible with the 7094. It also employed twos-complement arithmetic, but the exact product, quotient, and remainder in integer arithmetic survived. It was designed to be a very versatile machine with a complicated job control language, but its generality made it hard to use for simple tasks.

The first model of this machine we used at UCLA was the 360/91, which had a look-ahead feature as well as a stack (instruction cache). These gave the machine great speed when a program was written in machine language, since then branching and register loading could often be accomplished in no extra time.

A drawback in using a stack and look-ahead was that when two instructions were being executed at the same time and an error occurred, it was difficult to determine what had happened. This produced a rather mystical, interpretive feeling among the programmers who had to try to guess what had happened and how to fix it, instead of just taking a dump, finding out what had happened and then removing the errors.

The cycle time on this 360 was 60 nanoseconds. For fixed point, the add time was 1 cycle, multiply time 7 to 11 cycles and divide time about 37 cycles. For floating point, the add time was 1 or 2 cycles, multiply time 3 or 4 cycles and divide time 9 to 12 cycles. In addition, execution of instructions was overlapped, especially floating point instructions, so that for many purposes, even for computations with integers, the floating point instructions gave much faster computations.

The fine collection of software surrounding this machine included excellent file-management features, assemblers, compilers, editors and interpreters. Also, it was possible to use David Cantor's valuable multiple-precision integer subroutine package.

The main program run on this machine was written by Mike Morrison and JB. In this program, which is discussed in **2**(d) below, a great deal of auxiliary factoring was done by dividing by a fixed set of small primes. Unfortunately the designers of the 360 had given the machine rather slow fixed-point multiply and divide instructions, while making the double-length floating-point operations very fast. Evidently their rationale was that all really important scientific calculations involve only approximate numbers. Thus, when we wanted to divide by 3, say, we programmed the division in floating-point rather than in fixed-point because the former was several times faster. The programming of this required that the binary point end up in the correct position so the integer part could be properly recovered. This was greatly assisted by an interpreter which allowed for a single-step-at-a-time analysis of how the floating-point instructions worked.

This machine's large memory permitted us to use over a million bytes of memory in the crucial reduction stage of a very large matrix of bits that produced the factorizations of F_7, the first and most significant factorization done on this machine among dozens of others that appear in these tables.

After being used on the 360 at UCLA for several years, the factorization program was moved in 1973 to the 360/67 at DeKalb. The program was further developed by Marvin Wunderlich, who used his own multiple-precision integer package and who also devised an automatic submission feature which made the program fully automatic. In this improved form, one could merely submit the number to be factored and, after some time, collect the printout of factors along with some interesting statistical data.

In addition to this powerful program, another program called DOWNRUN was written to implement a primality test devised by JLS and Wunderlich [**98**]. These two programs, used together, have allowed us to bring these tables to their present advanced state. Free computer time at NIU has of course been invaluable, as has the enthusiastic sponsorship of JLS and his Foundation for Number Theory Computing. This Foundation and its supporters deeply influenced the development and promotion of fine computing in number theory during the 1970's.

The 360/75 at the University of Illinois was used by SSW in the table testing mentioned in section A above. Also, he used the DEC 10/KI in a two months' factoring rerun that covered the complete set of tables and discovered or rediscovered the factors up to 2^{35} in the tables. The number representation and set of DEC 10 instructions facilitated multiple-precision arithmetic in base 2^{35}. Since this computer is a dual processor, one processor could work full time for the two months on the factoring, while the other satisfied the time-sharing needs of most of the other users. Much of the information gleaned from these runs was put into final form in files at DeKalb, where a good editor (WILBUR) from Stanford was in use.

The IBM 4341 was used by SSW to factor some large numbers, such as 2,302M and $10^{56}+1$, by the continued fraction method. He also used the Illinois Central Editor (ICE) to perform the final testing on the tables. The factoring was done with “bulk time”, an arrangement whereby the interstitial time on the machine could be used essentially independently of other large projects.

The 360/91 at IBM at Yorktown Heights was used by BT for a search for Mersenne primes which discovered the prime M_{19937} [**102**]. The program that did this testing was written by BT with very careful thought to timing, in that the programs took advantage of the author’s detailed knowledge of instruction and hardware operation. To utilize the greater speed of the 360/91 on floating versus fixed point, the relevant programs were written, or rewritten, in floating point.

(k) *Other Computers.* A direct search for factors was carried out over many months on an IBM 1130 at the Mathematics Department at the University of Arizona. This small 16-bit word computer is quite slow by modern standards, but slow computers are often more widely available than fast ones. A common computer center policy is to permit a fast computer to be used only by funded researchers, so that one is given the option of having little or no time on a really fast computer or a great deal of time on a slow computer. The 1130 search found all the factors less than 2^{30} of 2^n-1 for various n for which a search had not earlier been completed.

At UC Berkeley, after the IBM 7094 was inactivated, a CDC 6400 became the main machine. This fast machine permitted several jobs to run side-by-side in the memory, which allowed for useful computing to be done on one program while another was inputting or outputting. A small zero-priority program, written by DHL and Peter Weinberger, was tucked away in the memory and was always available to continue its search for factors up to 10^{12} on a particular number. This valuable program produced many factors.

Since this program was to be as unobtrusive as possible, it was designed to take as little memory as possible, and so did its outputting by the following indirect procedure: when a factor was found, the program stored it in a particular memory location and then deliberately divided by zero. This produced an error condition that caused the system automatically to take a tiny dump of the part of the memory where the factor was stored. Fetching the factor from the dump in octal and converting it to decimal was a small matter, provided that the single sheet of output was not lost and was put in DHL’s output box.

One of the more interesting factorizations obtained by this background program was 698962539799.4096460559560875111, which finished off $2^{333}-1$.

An amusing by-product of having a program always in memory, ready to run whenever nothing else was running, was that the running time of the program accurately measured the idle time of the computer. Occasionally this caused comment when it was discovered that the program had run almost 100 percent of the time.

The hardware of this machine was poor for number theory in that on multiplying, it did not produce a double-word product. One had to do each multiplication twice to get the two product words.

The Swedish computer BESK was used by Hans Riesel for several purposes [**86** to **89**], among them the factoring of Mersenne numbers and the primality testing of these numbers.

The Illiac II was used by D. B. Gillies [**22**] to factor Mersenne numbers and to study the distribution of Mersenne primes.

DHL used the Illiac IV at Moffett Field, California, for factoring and primality testing. This interesting computer had a 64-bit word and a cycle time of 64 nanoseconds. An addition took 240 nanoseconds and a multiply took 400 on the individual processors. A very useful feature of this machine was its capability of carrying out the same operation on 64 numbers at the same time.

Hugh Williams has used an Amdahl 470/V7 for some of the more difficult primality testing and for the factorization of various large composite numbers by the two-step Pollard method [**80**].

Finally, Robert Baillie has obtained some impressive factorizations using idle time on the Plato system's CDC 6500 at the University of Illinois, and Hiromi Suyama has found factors of several Fermat and Mersenne numbers with his own 8-bit MZ-80C microcomputer.

Some more recent factorizations have also been included in the tables. (See the status report in section **IV B**.)

2. Developments in Factorization.

> "The problem of distinguishing prime numbers from composite numbers and of resolving the latter into their prime factors is known to be one of the most important and useful in arithmetic. It has engaged the industry and wisdom of ancient and modern geometers to such an extent that it would be superfluous to discuss the problem at length. Nevertheless we must confess that all methods that have been proposed thus far are either restricted to very special cases or are so laborious and prolix that even for numbers that do not exceed the limits of tables constructed by estimable men, i.e. for numbers that do not yield to artificial methods, they try the patience of even the practiced calculator... The dignity of the science itself seems to require that every possible means be explored for the solution of a problem so elegant and so celebrated." *C. F. Gauss* [**21**, Sec. 329]

In the past, before electronic computers, only a few factors of the numbers in these tables were discovered in a year's time, and a record was kept of who had discovered the factors. Computers have made factorization such a prolific activity that exhaustive documentation is, of course, no longer practicable. Accordingly, we mention only a few outstanding cases in this *Introduction* and make no attempt at all to document the tables themselves. A few factors in the tables have appeared earlier in privately circulated lists of E. Karst and M. Merson. (See [**6, 7, 30**].)

After the extensive searches for factors that we conducted, a final search by SSW put the tables in almost final form for publication. This was a direct search made after the compilation and distribution of a first version of the tables in 1976 to a few interested parties. In this search all the numbers in the tables were refactored up to a common search limit of 2^{35}. With the known factors having been rediscovered and the new factors entered in the tables, we are confident that the tables contain all prime factors less than 2^{35}.

In this section, we limit our discussion to the factoring methods we have actually used, since, as mentioned before, this is not a history of the subject, but rather an account of the building of these tables.

(a) *Direct Search.* This "divide and conquer" method (most often more divide than conquer) is a factoring method in which a sequence of trial divisors is generated, usually in order of increasing magnitude. Each member of the sequence, less than some factoring bound, is divided into the number N to see if it divides exactly.

The most common method of generating the sequence of trial divisors is with the use of an increment table. The increments in the table are the remaining differences after certain terms in the appropriate arithmetic sequence are sieved out because they are multiples of small primes. These primes usually don't exceed 13 because of space limitations in the computer [**92, 2**]. The table of increments is first constructed by the computer and is then used over and over again to create the sequence of trial divisors.

Although composite trial divisors remain in the sequence, it is more practical just to try them as possible divisors than to spend time eliminating them, unless trying one of them is very time-consuming. In [**26**] the authors found it better to use an extensive sieve and eliminate most composite numbers from the sequence of trial divisors.

Perhaps the simplest way to program the construction of the increment table is through the use of a GCD subroutine, which rejects a member of the arithmetic sequence to which the factors belong if it has a factor in common with any of the sieve primes. A good check on the increment table is to sum its entries. In the direct search to 2^{35}, SSW did not use an increment table. To seek small factors of $2^p - 1$, for example, he chose J so that $8pJ$ was a reasonable size, say $8pJ \approx 10^5$ with J the product of small odd primes. Then for each appropriate $S \leq 8pJ$ with $(S, J) = 1$, the trial divisors $f = S + 8pJk$, $k = 0, 1, 2, \ldots$, were tested in that order for $f < 2^{35}$. This strategy kept the memory requirements small. Here, "appropriate" means that if N has a particular form, the sequence to which the factors belong may be severely restricted. For example, if $N = 2^p - 1$, p prime, all factors are of the form $kp + 1$ and $8k \pm 1$. For another example, the possible prime factors q of $\Phi_n(b)$, apart from a possible intrinsic factor, must belong to the arithmetic progression $q \equiv 1 \pmod{n}$ if n is even, or $q \equiv 1 \pmod{2n}$ if n is odd. (See section **C**.)

A direct search is usually made to try to find small prime factors of N before anything else is done. When the factors less than the search bound are removed, then the remaining **cofactor** (again called N) is tested in Fermat's congruence to determine if N is composite or if N is a **probable prime**, i.e., a number that satisfies Fermat's congruence for some nontrivial base.

(b) *Legendre's Method.* In this method the sequence of trial divisors is obtained by using a much more elaborate sifting method, a quadratic sieve. By using quadratic residues of N, each prime factor of N is discovered to have certain numbers (usually primes) as quadratic residues. This implies that the prime factors of N lie in readily determined arithmetic sequences. By combining these, a sequence of trial divisors can be generated.

This method [**38, 75**, p. 198] was used by Jerry Johnson in 1963 to factor $N = 2^{101} - 1$, a number which had stood for decades as the Mersenne number whose factorization was "most wanted". In the IBM 704 program that factored it, prime quadratic residues of N were obtained from the continued fraction expansion of $\sqrt{mN}$ for various values of m. (See [**32**] for a discussion of this method.) The program that expanded $\sqrt{mN}$ and factored the denominators of the complete quotients also checked to see if any of these denominators was a square, just as hand calculators had done for decades. The occurrence of a square can sometimes give an immediate factorization of N.

(c) *Difference of Squares and Quadratic Forms.* The difference of squares method is one of the oldest factorization methods we have used. This method, introduced by Fermat, was improved by Gauss [**21**, Sec. 319–321]. (See [**42**] for a discussion of the use of this method on early sieves and [**6**] for its implementation on an electronic computer, and see also [**49, 50, 33**, Ch. VI].) Fermat would seek to find nontrivial x and y so that $x^2 - y^2 = N$, from which a factorization directly follows. Gauss wrote this equation as the congruence $y^2 \equiv x^2 - N \pmod{E}$ for various moduli E, thereby restricting the values of x to about one half of the possible residues modulo E. Combining these restrictions produced a sieve which excluded all values of x except for about one in 2^s when s exclusion moduli E were used. For some numbers with a special form such as $2^n - 1$, the x in this representation can be shown to lie in a certain arithmetic sequence. When this information is introduced at the outset as a change of variable, the sifting problem is considerably reduced [**45, 50**].

Since the difference of squares method works best when N can be expressed as a product of two factors of comparable size, it is sometimes better to factor mN, instead of N, for some value of m. (See [**39**] for a discussion of this old idea.) One then seeks values for x and y so that $y^2 \equiv x^2 - mN \pmod{E}$, again for various values of E. A sieve on x is then set up as before.

This method was used on all the sieve machines of DHL, one of the most impressive results being the DLS 127 factorization

$$\frac{2^{136}+1}{257.383521} = 2368179743873.373200722470799764577$$

[**7**, p. 644]. This problem was run on a standby basis on that sieve for 2600 hours before the number factored. Ten different multipliers m were used, the last, which did the job, being

$$m_{10} = 165670849 = 1 + 2^6.3^2.7.17.2417\,.$$

The sieve was run for only 12.5 hours with m_{10}. This sobering result shows all too well how little we knew (and still know) about choosing a good multiplier in this method.

In addition to the special case of a difference of squares, there is also Euler's factorization method of expressing N as a quadratic form in two different ways. This method was employed on the different sieves to good effect [**68, 48**, p. 106]. A still further method, using sets of forms, was developed in [**65**]. Generally speaking, however, sieve methods of factorization no longer compete with the continued fraction method. (See also [**48**].)

(d) *The Continued Fraction Method.* Experience with Legendre's method and an analysis of its arithmetical behavior suggested to JB that certain residues produced in the simple continued fraction expansion of $\sqrt{mN}$ might be multiplied together to produce a perfect square. This procedure (incorrectly called "Legendre's Method" in the first edition (1969) of [**32**]) contrasts with method (b) above, in which a square times a prime is sought. Although previous hand calculation with this method had shown that a square produced in this way quite often failed to lead to a factorization of N, it became apparent when this method was running at UCLA that it was, despite these failures, very much more powerful than any general factoring method that had been used before [**75**].

The ideas in this method had been discussed earlier from the point of view of the *failures* in the method by DHL and R. E. Powers [**46**], because as a hand method it continually failed to factor N despite a large amount of computation.

As the method was developed by Mike Morrison and JB, it also became apparent that a small set of primes was all that was needed in factoring the denominators of the complete quotients; most of the denominators were discarded when they did not factor enough with just these primes. This has been verified in general through the statistics that have been kept in recent years by Marvin Wunderlich. In private conversations, H. J. Godwin has also indicated that in his experience with the method, a small set of primes augmented by new primes that arise from completely factoring some of the denominators, seems to provide a growing factor base which is quite effective for the method.

Although the method often fails to factor N the first time that a square has been constructed, it almost always factors the number soon after the squares begin to appear. The power of the method can be illustrated by the factorization of $2^{128}+1$ [**73**], that of $2^{149}-1$ by Rich Schroeppel [**7**, p. 645], that of the 49-digit cofactor of $3^{121}-1$ by SSW, and by the fact that throughout these tables no composite number with 50 or fewer digits remains to be factored. (See **IV** for more recent information.) The main reason for this power is that all the auxiliary factoring is of numbers less than $2\sqrt{mN}$.

(e) *The Methods of John Pollard.* Two other methods, introduced by John Pollard, were of great importance in carrying out the factorizations in these tables. The first, or "$p-1$" method [**80**] is often spectacularly successful since it can sometimes find a quite enormous factor p with very little computing if $p-1$ splits entirely or almost entirely into a product of small primes.

The $p-1$ method may have one or two steps. Using only the first step, one finds a factor p, regardless of its size, if $p-1$ is a product of small primes. Using both steps, one finds a factor p if $p-1$ is a product of small primes and a single larger prime.

Both the single and double step methods have been programmed and have occasionally produced much larger factors than those which can be found by most other methods. For example, using only the single step method, we found the 19-digit factor $p = 1325815267337711173$ of $10^{53}-1$ in only a few minutes on the IBM 360/67, since $p-1 = 2^2.3^2.11.53.1279.1553.3557.8941$. Robert Baillie at the University of Illinois used the double step method to find the impressive 25-digit factor $p = 1155685395246619182673033$ of the 63-digit cofactor of the Mersenne number $2^{257}-1$ in about 50 minutes on the Plato system's CDC 6500, since $p-1 = 2^3.3^2.19^2.47.67.257.439.119173.1050151$. It was fortunate that the first step was taken at least up to 119173, for otherwise this factor of $2^{257}-1$ would not have been found. He has kindly permitted us to publish other factors he has found by this method.

A related method which can find prime factors p of N when $p+1$ factors completely into small primes, has been programmed by Earl Ecklund and JB at

DeKalb. The two step method for $p-1$ and $p+1$ has been programmed by Hugh Williams at Winnipeg. In this modification of Pollard's method the divisibility properties of Lucas sequences are used. The factors found by Williams are included here with his permission (two factors were found independently by G. J. Stevens).

It sometimes happens in this method that the smallest factor is not the first to be found. For example, the impressive 23-digit factor 53199025841281128499153 is the largest factor of $11^{59}+1$, and this was discovered before the two 17-digit factors.

The second method of Pollard [**81**], the so-called "Rho" or "Monte Carlo" method, has been used by the authors only in auxiliary factoring associated with primality testing. This powerful method was also used by M. Penk [**77**] to discover the factor 535006138814359 of $2^{257}-1$, the largest of the original Mersenne numbers and known to be composite for half a century. Richard Brent also used a variation of this method to factor the eighth Fermat number $F_8 = 2^{256}+1$, obtaining the factor 1238926361552897. The cofactor of F_8 was shown to be prime by Williams and Brent.

The factorization of $2^{191}-1$ is interesting in that it was accomplished through the use of four different factoring methods: besides the "Euler factor" 383, the second factor was then found by direct search; the fourth was found by Pollard $p-1$; the third and fifth were found using the continued fraction method. (The second factor could actually have been found much more readily using the Pollard $p-1$ method.)

There is little doubt that Pollard's methods will have great importance in further factorizations in these tables, since most composite numbers in these tables have not yet been attacked by either of these methods. (This work was done by the time of the second edition. See Section **IV A 2***(a)*.)

3. Developments in Primality Testing.

In this section we give an account of the primality tests that have been used in building these tables. This account is more detailed than that of the preceding section, because it is almost impossible, by studying the literature alone, to determine how these primality testing methods developed.

(a) *The Theory.* By a "primality test" we shall always mean a rigorous proof of primality, and not a probabilistic method for asserting the likelihood of primality. That is, by a "primality test" on a number N, we mean an algorithm whose steps consist of verifying the hypotheses of a theorem whose conclusion is "N is prime." Thus, finding that the results at each step of the algorithm are true for N, we conclude that N must be a prime.

(1) *Trial Division.* Certainly the oldest way to prove a number prime is to show by trial division that it has no nontrivial factor less than or equal to its square root. If, however, a number N is too large for trial division alone to be practical, one first asks whether N satisfies Fermat's congruence

$$a^{N-1} \equiv 1 \pmod{N} \tag{1}$$

for some base a, $1 < a < N-1$. Fermat's congruence is a necessary but not a sufficient condition for primality. If it holds for an odd $N > 1$, we call N a **probable prime** base a and write "PRP(a)" or just "PRP". Many authors, including ourselves, have previously used the misnomer "pseudoprime" for "probable prime". We now use "pseudoprime" only for a composite number satisfying (1).

When N satisfies (1), one should try to complete a primality test on N rather than try to factor it. There is almost no chance that it is composite. In practice such composite N are almost never encountered; but when they are, we greet these true novelties with pleasure and curiosity. (See [**6**, p. 91].) Recently Carl Pomerance, JLS and SSW [**82**, p. 1024] suggested that augmenting one Fermat test with one specific test of the Lucas type might be a fast test for primality. No composite number is known which passes this pair of tests, but they have not proved that no such number exists. All of the probable primes in the tables have passed this specific test, giving convincing evidence, but no final proof, that they are primes. The computing was done by SSW.

(2) *Fermat's Method.* Factoring methods generally rely upon exhaustive trials of values in certain sequences. The difference of squares factoring method discussed in **2**(c) provides an example.

Here $N = ab = x^2 - y^2$ where the nontrivial values of x lie in the interval $\sqrt{N} < x < \frac{1}{2}(B + \frac{N}{B})$, where B is the direct search bound. If no x in this interval gives a factor of N, then N must be a prime. Often whole collections of x values can be disposed of without trying them by imposing necessary conditions on x, as in the quadratic exclusion method (a quadratic sieve) of Gauss. An example of this method can be found in [**43**].

(3) *Euler's Method.* Euler showed that if an odd number N can be expressed as a sum of two squares in essentially only one way, then N is prime. This has been used as a means of testing for primality when the number of possible representations could be scanned completely.

(4) *Converses of Fermat's Congruence.* E. Lucas [**71**, p. 302; **72**, p. 441] published two somewhat ineffective converses of (1), but the first really effective converse theorems for testing primality were published by M. Kraitchik [**34**, p. 135] and DHL [**40**, p. 330].

> *Theorem 1.* If there exists an a for which $a^{N-1} \equiv 1$, but $a^{(N-1)/q} \not\equiv 1 \pmod{N}$ for each prime factor q of $N - 1$, then N is prime.

The effectiveness of this theorem for large N arises from the fact that the needed remainders can be calculated in roughly $\log_2 N$ multiplications and divisions [**60**, p. 124]. Although several bases may have to be tried among the numbers for which the Jacobi symbol $(a|N) = -1$ before a single a is found for which all the hypotheses of Theorem 1 are satisfied, the main difficulty in using the theorem is that all the prime factors q of $N - 1$ must be found; but when $N - 1$ could be factored, this theorem was often implemented. For example, the primality of the 49-digit factor N of $2^{179} - 1$ was proved, with $a = 19$, from

$$N - 1 = 2^4.3.5.7.41.163.179.643.919.43399.1071379.23262667.1159540629640123\,.$$

Using Theorem 1 at two levels [**4**] gave the primality of the 37-digit factor N of $2^{181} - 1$, since $N - 1 = 2.5.181.M$, where M, a probable prime base 19, can be proved to be prime from the factorization

$$M - 1 = 2.3.47.253567.811039.2293751.32910082955041\,.$$

The standard test for primality of the Fermat number $F_n = 2^{2^n} + 1$ is the subject of the next theorem.

> *Theorem 2.* (Pépin [**78**]) The Fermat number F_n is prime for $n \geq 1$ if and only if $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

This test is well suited to binary computers [**90**], and see [**40**], p. 334], for the powering is pure squaring and the reductions (mod F_n) can be accomplished without dividing by noting that

$$A.2^{2^n} + B = A(2^{2^n}+1) + (B-A) \equiv B - A \pmod{F_n}$$

(5) *Proth's Theorem.* In [**85**], E. Proth published the following important generalization of Pépin's theorem.

> *Theorem 3.* Let $N = k.2^n + 1$, where $1 \leq k < 2^n$. If $a^{(N-1)/2} \equiv -1 \pmod{N}$ for some a, then N is prime.

The importance of this theorem, beyond its immediate application to numbers of certain forms, is that the complete factorization of $N-1$ is not needed to finish a primality test on N.

Theorem 3 was used in [**3**] by DHL for the primality testing of the numbers $N = 2^p \pm 2^{(p+1)/2} + 1$, where p is prime. Here the power of 2 in $N-1$ is larger than the cofactor, so the test can be made by Proth's theorem. For example, the number $2^{457} - 2^{229} + 1$ was proved to be prime in this way.

Rather than computing the required remainders (mod N) directly, the reductions in powering were first made with respect to the intermediate modulus $2^{2p}+1 = (2^p - 2^{(p+1)/2}+1)(2^p + 2^{(p+1)/2}+1)$, using the scheme mentioned in (4), and then with respect to the actual modulus N.

Sometimes the algebraic form of N readily yields the factorization of $N-1$. For example [**3**], and see [**40**, p. 329] and [**54**]], for certain p, 5 divides $2^p \pm 2^{(p+1)/2}+1$ and the quotient N is a probable prime. For such p we then have

$$N - 1 = 4[2^{(p-1)/2} \mp 1][2^{(p-3)/2} \pm 1]/5\,.$$

(6) *Pocklington's Theorem.* This theorem of 1914 is of great importance in the primality testing of numbers which are not of any special form.

> *Theorem 4.* Suppose that $N-1 = q^n R$, where q is a prime and $q \nmid R$. If a is such that $a^{N-1} \equiv 1 \pmod{N}$ and $(a^{(N-1)/q}-1, N)$ $= 1$, then each prime factor p of N satisfies $p \equiv 1 \pmod{q^n}$.

Although this theorem does not mention primality explicitly, it does give valuable information about the form of possible factors of the probable prime N. This theorem is stronger than Theorem 1, for the condition $(a^{(N-1)q}-1, N) = 1$ is more stringent than the condition $a^{(N-1)/q} \not\equiv 1 \pmod{N}$.

The first and most immediate application of this theorem is to combine the modular conditions on p for different divisors of $N-1$. For instance, if q_1^m and q_2^n divide $N-1$ and the hypotheses in Theorem 4 are satisfied, then any prime factor of N will be congruent to $1 \pmod{q_1^m q_2^n}$. Accordingly, we have the following primality test.

> *Corollary 1.* Suppose $N-1 = FR$, where F is completely factored, $F > R$ and $(F,R) = 1$. If there exists an a for which $a^{N-1} \equiv 1 \pmod{N}$, but $(a^{(N-1)/q}-1, N) = 1$ for each prime factor q of F, then N is prime.

This result is a very practical primality test, which for large N almost certainly will show that N is prime when enough prime factors of $N-1$ have been found for their product F to exceed $R=(N-1)/F$. In fact, this corollary is a generalization of Theorem 3, where the factored part is just a power of 2.

This corollary was used in many of the primality tests for numbers in these tables. Moreover, Theorem 4 can sometimes be useful in showing that N is prime even when $F<R$. For, if F is not too small, a direct search can sometimes be made with the terms of the sequence $kF+1$ to show that N has no factor $\leq \sqrt{N}$. (Some divisors in this sequence can be eliminated in advance by sieving with small primes.) This method was used in [**40**] to show that $N=440334654777631$, the cofactor of $10^{27}-1$, is a prime. (The correct remainders mod N of $3^{(N-1)/5}$ and $3^{(N-1)/52189481}$ are 313433259338997 and 78523825886276 respectively.)

Another way to use the form of the factors of N in case $F<R$ is to introduce this information into a difference of squares factorization, with the hope of cutting the possible values of x to only a few or none. This method was introduced and used in [**40**], where, for example, the number $N=(10^{31}+1)/11=909090909090909090909090909091$ could be shown to be prime because of the fortunate factorization of $N-1=10(10^{30}-1)/11$. (See [**41, 43**] for other examples.)

(7) *Lucas' Theorem.* In 1878 [**71**, p. 302] E. Lucas published a theorem which permitted the complete factorization of $N+1$ to be used for primality testing in a way comparable to that of $N-1$. To do this he introduced a pair of second order recurring sequences (now called **Lucas sequences**) defined as follows:

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

where P and Q are integers. Also, we let $D=P^2-4Q$ and $\varepsilon_N=(D|N)$, where the latter is the Jacobi symbol. With this theorem made effective by using only prime divisors q as in Theorem 1, we have the theorem of DHL [**44**, p. 442].

> *Theorem 5.* If $N|U_{N-\varepsilon_N}$, but $N\nmid U_{(N-\varepsilon_N)/q}$ for each prime q dividing $N-\varepsilon_N$, then N is prime.

If P and Q, and therefore D, are chosen so that $\varepsilon_N=-1$, then the hypotheses relate to $N+1$. The choice of Lucas sequence here compares with the choice of base in the $N-1$ theorems. That is, one experiments with choices P and Q until the sequence allows all the hypotheses to be satisfied. This theorem requires the computation of remainders (mod N) for terms with large subscripts. Lucas sequences satisfy many useful identities. For example, to compute U_m (mod N) one can use

$$\begin{aligned} U_{2n} &= U_nV_n, \\ V_{2n} &= V_n^2-2Q^n, \\ U_{2n+1} &= (PU_{2n}+V_{2n})/2, \\ V_{2n+1} &= (DU_{2n}+PV_{2n})/2. \end{aligned}$$

The test in Theorem 5 was programmed by DHL for the IBM 7094 with $P=1$ and Q chosen so that $\varepsilon_N=-1$. This program was used to demonstrate the primality of the 24-digit factor N of $2^{109}-1$, using $Q=5$. Here

$N+1 = 2.3.67.83.233.M$, where M was shown to be prime by Theorem 1, with $a = 3$, from $M - 1 = 2.3.503.1801.7643.2693893$. The theorem was also used [**6**] at several levels to show the primality of the 38-digit factor N of $2^{131} - 1$. The factorization $N + 1 = 2.3.5.7^2.11^2.2711.N_1$ was used with $Q = 17$, the factor N_1 being shown prime with $Q = 29$ and $N_1 + 1 = 2.3^3.89^2.30211.N_2$, where N_2 is in turn shown to be prime with $Q = -1$ from the complete factorization $N_2 + 1 = 2^2.389.22901.46616380229$.

The most familiar use of Lucas sequences is for testing the primality of Mersenne numbers. This was initiated by Lucas [**71**, pp. 305, 316] and made into a simple test by DHL in [**44**, p. 443]; see also [**51**].

> *Theorem 6.* For p odd, the Mersenne number M_p is prime if and only if $M_p|S_{p-1}$, where $S_{n+1} = S_n^2 - 2$, $S_1 = 4$.

This test, like the one for Fermat numbers (Theorem 2), can be carried out without dividing, because $A.2^p + B = A(2^p - 1) + (A + B) \equiv A + B \pmod{M_p}$. This well-known Lucas-Lehmer test has been used for all the modern testing of these numbers [**90, 86, 28, 22, 102, 76, 101**].

(8) *A "Lucas-Pocklington" Theorem.* As Pocklington's theorem is so important, it was reasonable to look for an analogous theorem for Lucas sequences. This was proved by DHL [**44**, p. 443].

> *Theorem 7.* Let $N+1 = q^n R$ where q is prime and $q \nmid R$. If $\{U_n\}$ is a Lucas sequence for which $N|U_{N-\varepsilon_N}$ and $(U_{(N-\varepsilon_N)/q}, N) = 1$, then each prime factor p of N satisfies $p \equiv \pm 1 \pmod{q^n}$.

As in Theorem 5, we choose a sequence with $\varepsilon_N = -1$ so that $N + 1$ appears in the subscripts. However, in this theorem the factors p belong to the *two* residue classes $\pm 1 \pmod{q^n}$ for each prime divisor q in $N + 1$, which cannot be combined immediately into these two classes $\pmod{F}$, where F is the product of the moduli. In fact, it was long thought that if s of these congruences were combined by the Chinese remainder theorem, the best that could be said about a prime factor p of N was that it belonged to one of 2^s different residue classes $\pmod{F}$. This apparent difficulty blocked the development of Lucas analogues for theorems on the "minus" side [**44**, p. 443, footnote].

It therefore came as a considerable surprise when Mike Morrison [**74**] proved that even though there are 2^s possible ways of combining the individual congruences, it is nonetheless true that each prime factor p of N satisfies $p \equiv \pm 1 \pmod{F}$. The following result opened the way to developing the "plus" side theorems.

> *Theorem 8.* Suppose that $N + 1 = FR$, where F is completely factored and $(F, R) = 1$. If there exists a Lucas sequence $\{U_n\}$ for which $N|U_{N+1}$ and $(U_{(N+1)/q}, N) = 1$ for each prime factor q of F, then each prime divisor p of N satisfies $p \equiv \pm 1 \pmod{F}$.

We learned recently that a result equivalent to Theorem 8 appears in Riesel [**118**, page 59, Sats 3.7].

(9) *Change of Base or Sequence. The Extra 2.* In the summer of 1964, JLS and JB were working together at UCLA. Out of this collaboration came two important ideas in primality testing. The first is a theorem of JLS [**6**, p. 89].

> *Theorem 9.* If $N - 1$ is completely factored and for each q_i dividing $N - 1$ there exists an a_i for which $a_i^{N-1} \equiv 1 \pmod{N}$, but $a_i^{(N-1)/q_i} \not\equiv 1 \pmod{N}$, then N is prime.

This theorem is an improvement on Theorem 1, since if an a can be found for which $a^{N-1} \equiv 1 \pmod{N}$, but $a^{(N-1)/q} \not\equiv 1 \pmod{N}$ for a particular q, then that q has been settled once and for all regardless of what bases are used for the other q_i. Thus, it is no longer necessary to find a single base a for which all the hypotheses are satisfied. This idea carried over into all the other theorems on the minus side [**7**, pp. 621–623]. On the plus side, JB suggested that if a change in sequence were needed, then another Lucas sequence should be tried with the same D. This can easily be done by the transformations $P_1 = P + 2$ and $Q_1 = P + Q + 2$. Using these ideas, it was possible to develop "change of sequence" theorems on the plus side that paralleled the change of base theorems on the minus side [**7**, pp. 629–631].

The second idea has to do with an extra factor of 2 that JB inadvertently put in the modulus of a difference of squares sieve setup for factoring. When the factor was found, JLS proved by a parity argument that the extra 2 should indeed be there. Later JB proved the general rule [**6**, p. 89] "... the modulus can be increased by a factor of 2 if $(N-1)/n$ is odd." Although this extra two in the modulus made the search for x go twice as fast and is therefore a useful improvement in difference of squares factoring whenever it can be made, it was to play an important role in primality testing, where the double modulus gave a correct size remainder in the theory. (See [**7**, eqs. (9) and (19)].)

(10) *Introduction of the Search Bound.* In 1966, DHL found a way of introducing into primality theory the information that $N-1$ has no factor below a certain bound. In its original, unpublished form (it first appeared in [**7**, p. 625] in the midst of the ideas that are developed there) it was expressed as follows:

> *Theorem 10.* Let $N - 1 = FR$, where F is completely factored and $(F, R) = 1$. If there is an a for which $a^{N-1} \equiv 1 \pmod{N}$, $(a^F - 1, N) = 1$, and $(a^{(N-1)/q} - 1, N) = 1$ for each prime factor q of F, and if all the prime factors of R exceed $\sqrt{R/F}$, then N is prime.

Note that the new element here is the GCD condition $(a^F - 1, N) = 1$. It should be emphasized that $\sqrt{R/F}$ is a bound on the size of the factors of the *auxiliary* factorization of $N-1$ and not on N itself.

(11) *The Cube Root Theorem.* A major improvement in primality testing was introduced by JLS in 1970, when he analyzed difference of squares techniques in primality testing. He observed that if the first trial divisor did not divide N (highly unlikely since N was a probable prime), then the next one was so much larger that proof of primality required the factoring of $N-1$ only up to the cube root of N. What follows is an early form of this theorem.

> *Theorem 11.* Let $N - 1 = FR$, where F is completely factored and $(F, R) = 1$. Suppose there exists an a for which $a^{N-1} \equiv 1 \pmod{N}$ and $(a^{(N-1)/q} - 1, N) = 1$ for each prime factor q of F. Let $R = rF + s$, $1 \le s < F$, and suppose $N < 2F^3 + 2F$, $F > 2$. If r is odd, or if r is even and $s^2 - 4r \ne t^2$, then N is prime. Otherwise, $s^2 - 4r = t^2$ and
>
> $$N = [\tfrac{1}{2}(s-t)F + 1][\tfrac{1}{2}(s+t)F + 1].$$

It is clear that all the computations that are required in this theorem are practical, being either powers or GCD's. As soon as F becomes large enough during the factoring of $N-1$ for $2F^3+2F$ to exceed N, then the primality test can be completed. In all the improvements that have been mentioned so far, the thrust has been to eliminate unnecessary computing or to replace time-consuming factoring by powering or GCD's.

(12) *The Joint Paper of 1975.* The major plan in [**7**] was to use the factorization of $N+1$ in parallel to that of $N-1$. The many different ideas:

(a) Morrison's theorem on the "plus" side,

(b) change of base and change of Lucas sequence,

(c) the extra 2,

(d) the factor bound,

(e) the cube root theorem,

coalesced into the powerful **combined theorem** of JLS [**7**, Theorem 20 and its Corollary 11]. Further slight sharpening has resulted in the following form of the combined theorem.

> *Theorem 12.* Let $N-1=F_1R_1$ and $N+1=F_2R_2$, where F_1, F_2 are complete factorizations and R_1, R_2 are composite numbers with no factors less than B_1, B_2, respectively, and define $G=\max(B_1F_1, B_2F_2-1)$. If $N<GB_1B_2F_1F_2/2$, then N is prime if it passes the powering and GCD tests analogous to those of Theorems 7 to 11. The denominator 2 may be omitted if $N=4k+1$ and $B_1F_1>B_2F_2$ or if $N=4k-1$ and $B_2F_2>B_1F_1$.

(b) *The Programs.* Most of the numbers marked as primes in these tables have been shown to be prime by the program DOWNRUN. This program was written by JLS and Marvin Wunderlich and is used in conjunction with two auxiliary factoring routines whenever a more powerful factoring program than DOWNRUN is needed. The factoring routines are the continued fraction program of JB and Mike Morrison and a single step Pollard $p-1$ routine. The continued fraction program is the automated version due to Wunderlich that can factor a number of up to 43 digits in a couple of hours.

DOWNRUN begins its work by finding all factors of $N-1$ and $N+1$ below the direct search bound. These numbers are factored simultaneously. If no complete factorization of $N-1$ or of $N+1$ is found, then the product of their known factors, along with the bound, is tried in the inequalities of Theorems 10 or 12. If neither of the cofactors R_1, R_2 of $N\mp 1$ is a probable prime base 13, the direct search is continued to 10^6 and the same procedure is repeated.

If R_1 or R_2 is found to be a probable prime, then the program *goes down* and does not presently come back up to the same level again. Thus, it can happen when both R_1 and R_2 are probable primes and $R_1<R_2$ that the possibilities for R_2 are not explored because the program went down on the minus side and was not able to complete the primality test. There is an option in the program, however, that permits the user to select the side on which the program may go down.

The program is also set up to accept factoring hints to help it in completing the proof. The simple yet incomplete strategy used in DOWNRUN is based on the practical observation that all but the larger numbers will automatically be processed using this simple strategy. The larger numbers can then be handled by designing a more complicated strategy that can be implemented using the input control options of DOWNRUN. A detailed description of the simple strategy is given in [**98**].

The primes in the table with at most 25 digits were shown to be prime either by direct search up to their square roots or by DOWNRUN. Since testing for primality up to this number of digits turns out to be somewhat trivial when the auxiliary factoring goes up to 10^6, we have not said anything further about the primality of these numbers in the tables other than to list them in the main tables. Most primes and probable primes with more than 25 digits are listed in Appendix A. (See **VII** for more information.) The primality proof for each of the primes is summarized in Appendix B.

In the final stages of preparing these tables, the probable primes with at most 72 digits were sent to Hugh Williams, whose powerful testing program can often routinely settle the primality of numbers up to 80 or even more digits. His programs found that every large probable prime which we sent to him was prime.

These programs are based on the primality theory which Williams has developed beyond that detailed in [**7**]. In his important extensions [**107** to **111, 117**] he utilizes properties of extensions of Lucas' and Lehmer's functions, as well as the factors of the cyclotomic polynomials $N^2 + N + 1$, $N^2 + 1$ and $N^2 - N + 1$. His fine paper [**111**] on primality testing delineates these extensions in the setting in which they arise and contains what needs to be said about the form the theory has taken since the publication of [**7**]. Because it is a rather complete account of these matters, we refer the reader to these papers. Further extensions of this kind appear to require new ideas since the higher cyclotomic polynomials have not yet been shown to be readily applicable to primality testing. However, some work in this direction is now being done. See section **IV A 3**.

A few prime proof summaries based on proofs due to others have been included in Appendix B.

(c) *The Proof Summaries.* The notation in the proof summaries that are listed in Appendix B employs the following abbreviations and signs:

PPL Proth-Pocklington-Lehmer. The proof was made using Theorems 1, 2 and the Corollary in [**98**, p. 110] and the prime factors of $N-1$.

CMB Combined Theorem. The proof was made using Theorems 3 and 4 in [**98**, p. 110] and prime factors of $N-1$ and $N+1$. The extra 2, mentioned in Theorem 12, was used if needed.

BLS7 Theorem 7 of [**7**]. The proof was made using Theorem 11 above. (This notation was not used in the first edition. See **IV A 3**(c).)

p A prime factor $p > 10^6$, given as a "hint". It is followed by an M, P, F3, F4 or F6, indicating it is respectively a factor of $N-1$, $N+1$, N^2+N+1, N^2+1 or N^2-N+1 at some level. This factor, which was discovered by one of the auxiliary factoring programs, is input with the number to be tested and is used to complete the primality test.

Example. 34 10,49− 201457393P CMB
Here the hint is the prime 201457393 which is a factor of $N+1$.

(n) This notation, placed after PPL or CMB, indicates the direct search had to be taken to n, instead of the standard 10^6, in order to obtain a sufficiently large search bound to complete the proof.

Example. *115 3,287− 42521761M CMBF4F6(10**8)
The combined theorem proves the primality using a hint on the minus side. Some small factors of F4 and F6 and the factor bound 10^8 are used in the proof. (There were many proofs with search bounds $> 10^6$ in the first edition, but most were simplified in the second edition.)
(* This proof is due to Hugh Williams.)

−,+ A minus sign indicates the cofactor R_1 of $N-1$ is a probable prime base 13 and the program, after finishing its testing of N assuming that R_1 is a prime, *went down* and then showed that R_1 actually is a prime by carrying out a primality test on it. (See **3**(a)(4).) A plus sign means the same, but for the cofactor R_2 of $N+1$.

Example. 40 2,278M +−CMB
Here, after removal of the factors $2.3^2.5.157$ from $N+1$ (the plus sign), we obtain the probable prime

$$R_2 = 88546630665248948043897559039615307$$

and then with the removal of the factors 2.7.233 from $R_2 - 1$ (the minus sign), we have the probable prime

$$R = 27144889842197715525413108227963$$

which was proved to be prime using the combined theorem.

Example. 58 2,329− −+−−−−CMB
Here the program descended 6 times before it was able to complete the test on this 58-digit cofactor of $2^{329}-1$.

Examples. 50 10,190M 6129730457M −PPL
52 2,289− +80216641M CMB .
In the first example the hint is removed from $N-1$ and then the probable prime cofactor is tested for primality. In the second example, the hint is used only after the program goes down on the plus side.

Mersenne This Mersenne number has been proved prime by the standard test, Theorem 6, **3**(a)(7) above.

(5**58+1)/26 M This indicates that the prime $(5^{58}+1)/26$ is to be used as a hint on the minus side. There are also other hints of this type given in Appendix B, always for large numbers, where the primality test becomes easy with this information. Other examples, which vary slightly in format, are:

83	6,107+	Cofactor of 6**53 − 1 M CMB
89	2,447−	Alg.PPL See [7]
231	2,1149+	Factors of 2**382 − 1 PPL

Example. 178 2,745− Factors of 2**148−1 −−−1317031M
89165962987803776023M BLS7.
After factors dividing $N-1$, the program goes down three times on the minus side. The proof was completed by the Cube Root Theorem with two hints on the minus side.

C. Multiplicative Structure of $b^n \pm 1$.

1. Algebraic and Primitive Factors.

The way in which $b^n - 1$ factors is determined in part by the polynomial factorization

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \qquad n \geq 1, \tag{2}$$

where $\Phi_d(x)$ is the dth cyclotomic polynomial, given by the formula

$$\Phi_d(x) = \prod_{\delta|d} (x^\delta - 1)^{\mu(d/\delta)}$$

where μ is the Möbius function [**55**, p. 28]. Since $\Phi_d(x)$ is irreducible over the integers for $d \geq 1$, the polynomial factorization in (2) is complete. Of course, it does not follow that the factorization

$$b^n - 1 = \prod_{d|n} \Phi_d(b) \tag{3}$$

is complete, since the integer $\Phi_d(b)$ may not be prime.

(a) Let $n \geq 3$ be odd and let $1, d_1, \ldots, d_s$ be the proper divisors of n. Then the factorization (3) is presented in Table $b-$ in the format

$$n \quad (1, d_1, \ldots, d_s) \quad p_1 . p_2 \ldots$$

where $p_1 . p_2 \ldots$ is the product of the known factors of $\Phi_n(b)$, the **primitive part** in the factorization. The **algebraic part** is then $(b^n - 1)/\Phi_n(b)$. The divisor $d = 1$ is omitted from the parentheses in Table 2$-$, because the factor $\Phi_1(2) = 1$ is trivial.

Since in this format a factor $\Phi_d(b)$ with $d < n$ is indicated only by its subscript, each of its prime factors needs to be entered only once in the table (after the parentheses on line d), rather than throughout the table at each place where $\Phi_d(b)$ occurs.

A prime divisor p of $b^n - 1, n \geq 2$, is called **primitive** if $p \nmid b^k - 1$ for any $k < n$. Otherwise, it is called **algebraic**. It is clear that any prime p dividing $\Phi_d(b)$ in (3) for $d < n$ will be algebraic, since then p will divide $b^d - 1$ because $\Phi_d(b)$ does. On the other hand, any primitive factor of $b^n - 1$ will have to divide the primitive part $\Phi_n(b)$. It is not true, however, that every prime factor of $\Phi_n(b)$ is primitive. An algebraic prime factor of $\Phi_n(b)$ is called **intrinsic** and is indicated in the main tables by an asterisk, except when $p = n = 2$. For example, $\Phi_{21}(2) = 7*.337$. Note that 7 divides $2^3 - 1$, so 7 is an algebraic factor of $\Phi_{21}(2)$.

A primitive prime divisor p of $b^n - 1$ is said to have **rank** n, and we write $r(p) = n$. A prime p is an intrinsic factor of $\Phi_m(b)$ if and only if $m = p^k r(p), k \geq 1$. Furthermore, when p is intrinsic, it divides $\Phi_m(b)$ just once, if $m > 2$.

(b) To find the factorization of $b^{2n} - 1 = (b^n - 1)(b^n + 1)$ requires the table of the factorizations of $b^n + 1, n \geq 1$. Thus, writing $2n = 2^t m, m$ odd, and using (2), we obtain

$$x^n + 1 = (x^{2n} - 1)/(x^n - 1) = \prod_{d|2n} \Phi_d(x) / \prod_{d|n} \Phi_d(x),$$

so

$$x^n + 1 = \prod_{d|m} \Phi_{2^t d}(x).$$

This result shows that the primitive part of $b^n + 1$ is $\Phi_{2n}(b)$, and

$$b^n + 1 = \prod_{d|m} \Phi_{2^t d}(b). \tag{4}$$

If the proper divisors of m are $1, d_1, \ldots, d_s$, then, since $\Phi_{2n}(b)$ is the primitive part of $b^n + 1$, the factorization in (4) is given in Table $b+$ in the format

$$n \quad (2^{t-1}, 2^{t-1}d_1, \ldots, 2^{t-1}d_s) \quad p_1 . p_2 \ldots$$

where as before $p_1 . p_2 \ldots$ is the product of the known prime factors of $\Phi_{2n}(b)$.

It should be noted that the very long table for the factorization of $2^n + 1$ has been broken into three tables, as in the earlier tables [**11**], which give the factorization of $2^{2k-1} + 1, 2^{4k-2} + 1$ and $2^{4k} + 1$. They are labeled respectively "Table 2+ (odd)", "Table 2LM" and "Table 2+(4k)". For each other base b, however, there is only the single "Table b+".

2. Aurifeuillian Factorizations.

For each base b, certain of the numbers $b^n \pm 1$ factor in a way different from the factorization obtained in (3) or (4). This second factorization is due to the existence of special polynomial identities, discovered by and named after Aurifeuille [**11**, p. v]. These identities show how to write $\Phi_n(x)$ in a form which becomes a difference of squares when x has certain values. In particular, putting $x = 2^{2k-1}$ in the identity

$$x^2 + 1 = \Phi_2(x^2) = (x+1)^2 - 2x$$

yields the factorization

$$2^{4k-2} + 1 = (2^{2k-1} - 2^k + 1)(2^{2k-1} + 2^k + 1). \tag{5}$$

Similarly, replacing x by 3^{2k-1} and 12^{2k-1} in the identity

$$x^3 + 1 = (x+1)\Phi_3(-x) = (x+1)[(x+1)^2 - 3x]$$

yields the factorizations

$$3^{6k-3} + 1 = (3^{2k-1} + 1)(3^{2k-1} - 3^k + 1)(3^{2k-1} + 3^k + 1) \tag{6}$$

and

$$12^{6k-3} + 1 = (12^{2k-1} + 1)(12^{2k-1} - 2^{2k-1}3^k + 1)(12^{2k-1} + 2^{2k-1}3^k + 1). \tag{7}$$

For compactness we write formulas (5), (6), (7) with $h = 2k - 1$ as

$$2^{2h} + 1 = \mathrm{L}_{2h}\mathrm{M}_{2h} \qquad 3^{3h} + 1 = (3^h + 1)\mathrm{L}_{3h}\mathrm{M}_{3h} \qquad 12^{3h} + 1 = (12^h + 1)\mathrm{L}_{3h}\mathrm{M}_{3h}$$

where

$$\mathrm{L}_{2h},\ \mathrm{M}_{2h} = 2^h + 1 \mp 2^k \quad\text{and}\quad \mathrm{L}_{3h},\ \mathrm{M}_{3h} = 3^h + 1 \mp 3^k \quad\text{or}\quad 12^h + 1 \mp 2^h 3^k.$$

In the same way we may set $x = 5^h, 6^h, 7^h, 10^h$ and 11^h in the respective identities

$$\begin{aligned}
x^5 - 1 &= (x-1)\Phi_5(x) = (x-1)[(x^2+3x+1)^2 - 5x(x+1)^2]\\
x^6 + 1 &= (x^2+1)\Phi_6(x^2) = (x^2+1)[(x^2+3x+1)^2 - 6x(x+1)^2]\\
x^7 + 1 &= (x+1)\Phi_7(-x) = (x+1)[(x+1)^6 - 7x(x^2+x+1)^2]\\
x^{10} + 1 &= (x^2+1)\Phi_{10}(x^2) \quad\text{and}\quad x^{11}+1 = (x+1)\Phi_{11}(-x)
\end{aligned}$$

$$\text{where}\quad \Phi_{10}(x^2) = (x^4+5x^3+7x^2+5x+1)^2 - 10x(x^3+2x^2+2x+1)^2$$

$$\text{and}\quad \Phi_{11}(-x) = (x^5+5x^4-x^3-x^2+5x+1)^2 - 11x(x^4+x^3-x^2+x+1)^2$$

and obtain the factorizations

(8) $5^{5h}-1 = (5^h-1)\mathrm{L}_{5h}\mathrm{M}_{5h}, \quad \mathrm{L}_{5h}, \mathrm{M}_{5h} = 5^{2h}+3.5^h+1\mp 5^k(5^h+1)$

(9) $6^{6h}+1 = (6^{2h}+1)\mathrm{L}_{6h}\mathrm{M}_{6h}, \quad \mathrm{L}_{6h}, \mathrm{M}_{6h} = 6^{2h}+3.6^h+1\mp 6^k(6^h+1)$

(10) $7^{7h}+1 = (7^h+1)\mathrm{L}_{7h}\mathrm{M}_{7h}, \quad \mathrm{L}_{7h}, \mathrm{M}_{7h} = (7^h+1)^3\mp 7^k(7^{2h}+7^h+1)$

(11) $10^{10h}+1 = (10^{2h}+1)\mathrm{L}_{10h}\mathrm{M}_{10h}, \qquad \text{where} \quad \mathrm{L}_{10h}, \mathrm{M}_{10h}$

$= 10^{4h}+5.10^{3h}+7.10^{2h}+5.10^h+1\mp 10^k(10^{3h}+2.10^{2h}+2.10^h+1)$

(12) $11^{11h}+1 = (11^h+1)\mathrm{L}_{11h}\mathrm{M}_{11h}, \qquad \text{where} \quad \mathrm{L}_{11h}, \mathrm{M}_{11h}$

$= 11^{5h}+5.11^{4h}-11^{3h}-11^{2h}+5.11^h+1\mp 11^k(11^{4h}+11^{3h}-11^{2h}+11^h+1).$

The appropriate formulas for L and M are also given at the end of each relevant main table.

The binomials with an Aurifeuillian factorization can be completely factored more readily than most other $b^n \pm 1$, because they break into two roughly equal pieces. For this reason, Table 2LM has been extended to 2400, twice as far as the other base 2 tables. The Aurifeuillian factorizations for the larger bases (in Tables 3+, 5−, 6+, 7+, 10+, 11+ and 12+) are not given in a separate table, but are incorporated in a special format in the tables themselves and are carried somewhat farther than the consecutively indexed entries, the extensions being listed below a line of dashes in the respective tables. (The line of dashes is omitted if it comes at a page boundary.)

Since the factorizations produced in (5) to (12) cut across those produced in (3) and (4), it is important to analyze how the two factorizations relate to each other.

Example 1. Since $156 = 2^2.39$, we have from (4) that

$$\begin{aligned}
2^{78}+1 &= \prod_{d|39}\Phi_{4d}(2) = \Phi_4(2)\Phi_{12}(2)\Phi_{52}(2)\Phi_{156}(2)\\
&= (5)(13)(53.157.1613)(\underline{13}{*}.\underline{313}.\underline{1249}.\underline{3121}.\underline{21841})
\end{aligned}$$

and from (5) that

$$2^{78}+1 = \mathrm{L}_{78}\mathrm{M}_{78} = (13.53.157.\underline{13}{*}.\underline{313}.\underline{1249})\,(5.1613.\underline{3121}.\underline{21841}).$$

The fact that the second factorization splits both the algebraic and primitive parts of $2^{78}+1$ suggests that in order to describe this multiplicative structure, the primitive parts of L_n and M_n should be defined so that L_n and M_n can be expressed as a product of primitive parts as in (3). To do this we denote the respective primitive parts by L_n^* and M_n^*. For base b, let $\varepsilon_d = \varepsilon_d(b) = [1+(b|d)]/2$, where d is odd, $(b,d)=1$ and $(b|d)$ is the Jacobi symbol. (Recall that $(b|1)=1$.) Also, let $n = 2^s m$, m odd, $s \geq 0$. Then we have the formulas (which we state without proof)

$$\mathrm{L}_n^* = {\prod_{d|m}}' [(\mathrm{L}_{n/d})^{\varepsilon_d}(\mathrm{M}_{n/d})^{1-\varepsilon_d}]^{\mu(d)} \tag{13}$$

and

$$\mathrm{M}_n^* = {\prod_{d|m}}' [(\mathrm{L}_{n/d})^{1-\varepsilon_d}(\mathrm{M}_{n/d})^{\varepsilon_d}]^{\mu(d)}, \tag{14}$$

so that

$$\mathrm{L}_n = {\prod_{d|m}}' [(\mathrm{L}_{n/d}^*)^{\varepsilon_d}(\mathrm{M}_{n/d}^*)^{1-\varepsilon_d}] \tag{15}$$

and

$$\mathrm{M}_n = {\prod_{d|m}}' [(\mathrm{L}_{n/d}^*)^{1-\varepsilon_d}(\mathrm{M}_{n/d}^*)^{\varepsilon_d}]. \tag{16}$$

In each case the prime on the product sign indicates that the product is taken over the divisors d of m such that $(b,d)=1$. It is easily shown that $\Phi_{4n}(b) = \mathrm{L}_{2n}^*\mathrm{M}_{2n}^*$ for odd n and that $(\mathrm{L}_n^*, \mathrm{M}_n^*) = 1$.

In Table 2LM (as in the other Aurifeuillian tables) we write the subscript n as a line number in front of L and M for ease of use, and list the L's and M's on the right of (15) and (16) with $d < m$ inside parentheses and the known prime factors of the primitive part after the parentheses as before. (In the first column of this table the line number $4k-2$ is written only in front of the L, not the M). Hence, using (13) to (16), the first five pairs of lines of Table 2LM would be:

2L 1	6L (2M) 1	10L (2M) 5*	14L (2L) 113	18L (2L,6M) 37
M 5	M (2L) 13	M (2L) 41	M (2M) 29	M (2M,6L) 109

Now, since $\mathrm{L}_2^* = \mathrm{L}_6^* = 1$, we can simplify the presentation by omitting 2L and 6L and writing 2 and 6 for M_2^* and M_6^*. These five pairs of lines then become:

2 5	6 (2) 13	10L (2) 5*	14L 113	18L (6) 37
		M 41	M (2) 29	M (2) 109

The other simplification of this kind that can be made in the Aurifeuillian tables is in Table 3+, where the entry

3	(1) L.M
L	1
M	7

is abbreviated as 3 (1) 7.

Example 2. With $b = 2$ and $n = 78 = 2.39$ we have from (15) that

$$\begin{aligned} \text{(17)} \qquad \mathrm{L}_{78} &= \prod_{d|39}{}' [(\mathrm{L}^*_{78/d})^{\varepsilon_d}(\mathrm{M}^*_{78/d})^{1-\varepsilon_d}] = \mathrm{L}^*_2.\mathrm{M}^*_6.\mathrm{M}^*_{26}.\mathrm{L}^*_{78} \\ &= (1)(13)(53.157)(\underline{13}^*.\underline{313}.\underline{1249}), \end{aligned}$$

since $\mathrm{M}^*_6 = \mathrm{M}_6/\mathrm{L}_2 = 13$ and $\mathrm{M}^*_{26} = \mathrm{M}_{26}/\mathrm{L}_2 = 53.157$. Also, by interchanging L and M in (17) we obtain immediately

$$\mathrm{M}_{78} = \mathrm{M}^*_2.\mathrm{L}^*_6.\mathrm{L}^*_{26}.\mathrm{M}^*_{78} = (5)(1)(1613)(\underline{3121}.\underline{21841}),$$

since $\mathrm{L}^*_{26} = \mathrm{L}_{26}/\mathrm{M}_2 = 1613$. These factorizations are given in Table 2LM as

$$\begin{array}{rll} \text{78L} & \text{(6,26M)} & 13{*}.313.1249 \\ \text{M} & \text{(2,26L)} & 3121.21841. \end{array}$$

Note here that $\mathrm{L}^*_{78}.\mathrm{M}^*_{78} = \Phi_{156}(2)$, as it should.

For $b > 2$, formulas (6) to (12) are given in a three-line format:

$$\begin{array}{rll} n & (\ldots) & \mathrm{L.M} \\ \mathrm{L} & (\ldots) & \mathrm{L}^*_n \\ \mathrm{M} & (\ldots) & \mathrm{M}^*_n \end{array}$$

where the first line contains the triple product in (6) to (12) and the second and third lines give the factorizations of the L and M indicated in the first line.

Example 3. With $b = 6$ and $n = 210$, we have from (9), (13) and (14) that

$$\mathrm{L}_{210} = \prod_{d|35}{}' [(\mathrm{L}^*_{210/d})^{\varepsilon_d}(\mathrm{M}^*_{210/d})^{1-\varepsilon_d}], \text{ where } \varepsilon_d = [1 + (6|d)]/2.$$

Thus, $\mathrm{L}_{210} = \mathrm{M}^*_6.\mathrm{M}^*_{30}.\mathrm{L}^*_{42}.\mathrm{L}^*_{210}$ and therefore we have directly

$$\mathrm{M}_{210} = \mathrm{L}^*_6.\mathrm{L}^*_{30}.\mathrm{M}^*_{42}.\mathrm{M}^*_{210}.$$

Hence, the factorization of $6^{210} + 1 = (6^{70} + 1)\ \mathrm{L}_{210}\mathrm{M}_{210}$ is given in Table 6+ as

$$\begin{array}{rll} 210 & \text{(2,10,14,70)} & \mathrm{L.M} \\ \mathrm{L} & \text{(6M,30M,42L)} & \mathrm{L}^*_{210} \\ \mathrm{M} & \text{(6L,30L,42M)} & \mathrm{M}^*_{210}\,. \end{array}$$

Here the decomposition of the algebraic factor $6^{70} + 1$ is of course obtained from (4).

In computing L^*_n and M^*_n the following "crossover" theorem [**36**, p. 181; **37**, p. 46] is sometimes useful. Assume that $(b, k) = 1$.

$$\text{If } (b|k) = +1,\ \mathrm{L}_n \text{ divides } \mathrm{L}_{kn} \text{ and } \mathrm{M}_n \text{ divides } \mathrm{M}_{kn}.$$

$$\text{If } (b|k) = -1,\ \mathrm{L}_n \text{ divides } \mathrm{M}_{kn} \text{ and } \mathrm{M}_n \text{ divides } \mathrm{L}_{kn}.$$

D. Acknowledgements.

Many persons have contributed to these tables in the long period of time in which they have been built up. Among these we would especially like to thank David Cantor, Robert Coffin, René De Vogelaere, Earl Ecklund, Richard Guy, Alexander Hurwitz, Paul Morton, John M. Pollard, Raphael Robinson, Richard Schroeppel, Henry Thomas, Vance Vaughan, and Peter Weinberger.

The impressive results of the last twenty-five years would not have been obtained without easy access to computers. Accordingly we would like to express our gratitude to the directors and the staffs of the following computing establishments: Mathematics Department, University of Arizona; Bell Telephone Laboratories, Murray Hill; The Computer Center, UC, Berkeley; IBM, Yorktown Heights; Northern Illinois University; University of Illinois; The Computer Center, Stanford University; and the Computing Facility, UCLA.

There are four persons we would like to single out for special thanks. The first is Hugh Williams, whose assistance in the final stages of factoring and primality testing of large "hold-outs" has been most helpful. The second is Mike Morrison, who has assisted us at several stages of the work and who set up at Northern Illinois University the factoring program which he and JB developed at UCLA. This program, and its later automatic version due to Marvin Wunderlich and SSW, were of signal importance in much of our primality testing, as well as in the factoring of all composite numbers in the tables with no more than 50 digits.

The third person is Marvin Wunderlich, who has been so energetic in developing, maintaining and using the factorization program and the primality testing program DOWNRUN at DeKalb in conjunction with JLS. His work with the authors and with the Cunningham Project stands behind many of the results here, not the least of which is the collection of primality proofs in Appendix B, a large portion of which are due to DOWNRUN.

The fourth person is Emma Lehmer, who, except for her insistence to the contrary, would have been listed among the authors of this work. To have worked with her and thereby to have benefited from her cheerful and effective involvement in all the stages of this work has put us very much in her debt. We wish to express our deep appreciation to her.

References

1. N. G. W. H. Beeger, MTAC **4** (1950), 124.
2. John Brillhart and G. D. Johnson, *On the Factors of Certain Mersenne Numbers*, Math. Comp. **14** (1960), 365–369, MR **23** #A832.
3. John Brillhart, *Concerning the Numbers* $2^{2p}+1$*, p Prime*, Math. Comp. **16** (1962), 424–430, MR **26** #6100.
4. John Brillhart, *Some Miscellaneous Factorizations*, Math. Comp. **17** (1963), 447–450.
5. John Brillhart, *On the Factors of Certain Mersenne Numbers, II*, Math. Comp. **18** (1964), 87–92, MR **28** #2992.
6. John Brillhart and J. L. Selfridge, *Some Factorizations of* $2^n \pm 1$ *and Related Results*, Math. Comp. **21** (1967), 87–96; Corrigendum, *ibid.*, 751, MR **37** #131.
7. John Brillhart, D. H. Lehmer, and J. L. Selfridge, *New Primality Criteria and Factorizations of* $2^m \pm 1$, Math. Comp. **29** (1975), 620–647, MR **52** #5546.
8. R. D. Carmichael, *On the Numerical Factors of the Arithmetic Forms* $\alpha^n \pm \beta^n$, Annals of Math. (2) **15** (1913-1914), 30–70.
9. R. D. Carmichael, *Fermat Numbers* $F_n = 2^{2^n}+1$, Amer. Math. Monthly **26** (1919), 137–146.
10. Carnegie Institution of Washington, News Service Bulletin (School Edition), III, No. 3, March 12, 1933, 19–22.
11. A. J. C. Cunningham and H. J. Woodall, *Factorisation of* $y^n \mp 1$*,* $y = 2, 3, 5, 6, 7, 10, 11, 12$ *Up to High Powers* (n), Hodgson, London, 1925.
12. L. E. Dickson, *History of the Theory of Numbers*, Chelsea, New York, 1952, Ch. XIV.
13. John D. Elder, *Errata in the Lehmer Factor Stencils*, Bull. Amer. Math. Soc. **43** (1937), 253–255.
14. A. Ferrier, *A New Factorization of* $2^n + 1$, MTAC **3** (1949), 451.
15. A. Ferrier, *Note on the Factors of* $2^n + 1$, MTAC **3** (1949), 496–497, MR **11**, 11.
16. A. Ferrier, *New Factorizations of* $2^n \pm 1$, MTAC **4** (1950), 54–55.
17. A. Ferrier, *On Large Primes and Factorizations III*, MTAC **4** (1950), 124–125; Corrigendum, *MTAC* **5** (1951), 259.
18. A. Ferrier, *On the Number* $2^{151} + 1$, MTAC **5** (1951), 55.
19. A. Ferrier, *The Determination of a Large Prime*, MTAC **6** (1952), 256.
20. E. Gabard, *Factorization d'un Nouveau Nombre de Mersenne*, Mathesis (1959), 61.
21. C. F. Gauss, *Disquisitiones Arithmeticae*, tr. by A. A. Clarke, S. J., Yale University Press, 1966, MR **33** #5545.
22. Donald B. Gillies, *Three New Mersenne Primes and a Statistical Theory*, Math. Comp. **18** (1964), 93–95.
23. G. Gostin, *A Factor of* F_{17}, Math. Comp. **35** (1980), 975–976, MR 81f:10010.
24. Richard K. Guy, *How to Factor a Number*, Congressus Numerantium **16** (1976), 49–89, MR **53** #7924.
25. Marshall Hall, *Quadratic Residues in Factorization*, Bull. Amer. Math. Soc. **39** (1933), 951–953.
26. John C. Hallyburton and John Brillhart, *Two New Factors of Fermat Numbers*, Math. Comp. **29** (1975), 109–112; Corrigendum, *Math. Comp.* **30** (1976), 198, MR **52** #13599.
27. Alexander Hurwitz and J. L. Selfridge, *Fermat Numbers and Perfect Numbers*, AMS Notices **8** (1961), 601.
28. Alexander Hurwitz, *New Mersenne Primes*, Math. Comp. **16** (1962), 249–251, MR **26** #3684.
29. K. R. Isemonger, *The Complete Factorization of* $2^{132} + 1$, Math. Comp. **14** (1960), 73–74, MR **22** #22.
30. K. R. Isemonger, *Complete Factorization of* $2^{159} - 1$, Math. Comp. **15** (1961), 295–296, MR **23** #A1577.
31. K. R. Isemonger, *Some Additional Factorizations of* $2^n \pm 1$, Math. Comp. **19** (1965), 145–146, MR **30** #1081.
32. D. Knuth, *The Art of Computer Programming,* v. 2, *Seminumerical Algorithms*, Addison-Wesley, Reading, Mass., 1969 (1st ed.), 1981 (2nd ed.), MR **44** #3531 and 83i:68003.
33. M. Kraitchik, *Théorie des Nombres*, Gauthier-Villars, Paris, 1922, Ch. 2.
34. M. Kraitchik, *Théorie des Nombres,* Tome 2, Gauthier-Villars, Paris, 1926.
35. M. Kraitchik, *Recherches sur la Théorie des Nombres,* Tome 2, Gauthier-Villars, Paris, 1929.

36. M. Kraitchik, *Introduction à la Théorie des Nombres*, Gauthier-Villars, Paris, 1952, MR **14**, 535.
37. M. Kraitchik, *On the Factorization of* $2^n \pm 1$, Scripta Math. **18** (1952), 39–52, MR **14**, 121.
38. A. M. Legendre, *Théorie des Nombres,* Tome 1, 3rd ed., Paris, 1830, pp. 334–341; *Zahlentheorie*, tr. by H. Maser, Teubner, Leipzig, 1893, pp. 329–336.
39. R. Sherman Lehman, *Factoring Large Integers*, Math. Comp. **28** (1974), 637–646, MR **49** #4919.
40. D. H. Lehmer, *Tests for Primality by the Converse of Fermat's Theorem*, Bull. Amer. Math. Soc. **33** (1927), 327–340.
41. D. H. Lehmer, *A Further Note on the Converse of Fermat's Theorem*, Bull. Amer. Math. Soc. **34** (1928), 54–56.
42. D. H. Lehmer, *The Mechanical Combination of Linear Forms*, Amer. Math. Monthly **35** (1928), 114–121.
43. D. H. Lehmer, *On the Number* $(10^{23} - 1)/9$, Bull. Amer. Math. Soc. **35** (1929), 349–350.
44. D. H. Lehmer, *An Extended Theory of Lucas' Functions*, Annals of Math. (2) **31** (1930), 419–448.
45. D. H. Lehmer, *On the Factorization of Lucas' Functions*, Tôhoku Math. J. **34** (1931), 1–7.
46. D. H. Lehmer and R. E. Powers, *On Factoring Large Numbers*, Bull. Amer. Math. Soc. **37** (1931), 770–776.
47. D. H. Lehmer, *Note on Mersenne Numbers*, Bull. Amer. Math. Soc. **38** (1932), 383–384.
48. D. H. Lehmer, *Some New Factorizations of* $2^n \pm 1$, Bull. Amer. Math. Soc. **39** (1933), 105–108.
49. D. H. Lehmer, *A Photo-electric Number Sieve*, Amer Math. Monthly **40** (1933), 401–406.
50. D. H. Lehmer, *A Machine for Combining Sets of Linear Congruences*, Math. Annalen **109** (1934), 661–667.
51. D. H. Lehmer, *On Lucas' Test for the Primality of Mersenne's Numbers*, J. London Math. Soc. **10** (1935), 162–165.
52. D. H. Lehmer, *On the Converse of Fermat's Theorem*, Amer. Math. Monthly **43** (1936), 347–354.
53. D. H. Lehmer, *Sur les Essais Directs de Primalité*, Sphinx **8** (1938), 87–88.
54. D. H. Lehmer, *A Factorization Theorem Applied to a Test for Primality*, Bull. Amer. Math. Soc. **45** (1939), 132–137.
55. D. H. Lehmer, *Guide to Tables in the Theory of Numbers*, National Research Council, Washington D. C., 1941, MR **2**, 247.
56. D. H. Lehmer, *On the Factors of* $2^n \pm 1$, Bull. Amer. Math. Soc. **53** (1947), 164–167, MR **8**, 441.
57. D. H. Lehmer, *On the Converse of Fermat's Theorem, II*, Amer. Math. Monthly **56** (1949), 300–309, MR **10**, 681.
58. D. H. Lehmer, *Two New Mersenne Primes*, Amer. Math. Monthly **7** (1953), 72.
59. D. H. Lehmer, *An Announcement Concerning the Delay Line Sieve DLS 127*, Math. Comp. **20** (1966), 645–646.
60. D. H. Lehmer, *Computer Technology Applied to the Theory of Numbers*, Studies in Number Theory, MAA Studies in Math., v. 6, 1969, pp. 117–151, MR **40** #84.
61. D. H. Lehmer, *The Economics of Number Theoretic Computation*, Computers in Number Theory, ed. by A. O. L Atkin and B. J. Birch, Academic Press, 1971, pp. 1–9.
62. D. H. Lehmer, *The Influence of Computing on Research in Number Theory*, The Influence of Computing on Mathematical Research and Education, Proc. of Symposium in Applied Math., v. 20, Amer. Math. Soc., 1974, 3–12, MR **51** #316.
63. D. H. Lehmer, *Exploitation of Parallelism in Number Theoretic and Combinatorial Computation*, Proc. of the Sixth Manitoba Conf. on Numerical Math. (1976), 95–111, MR **58** #27706.
64. D. H. Lehmer, *A History of the Sieve Process*, *A History of Computing in the Twentieth Century*, Los Alamos, 1979, pp. 445–456, MR 81i:68002.
65. D. H. Lehmer and Emma Lehmer, *A New Factorization Technique Using Quadratic Forms*, Math. Comp. **28** (1974), 625–635, MR **49** #7204.
66. D. N. Lehmer, *On the History of the Problem of Separating a Number into Its Prime Factors*, Scientific Monthly (Sept. 1918), 227–234.
67. D. N. Lehmer, *On a New Method of Factorization*, Proc. Nat. Acad. Sci. **11** (1925), 97–98.

68. D. N. Lehmer, *Hunting Big Game in the Theory of Numbers*, Scripta Math. **1** (1932-33), 229–235.
69. D. N. Lehmer, “Factor Stencils”, Revised and Extended by John D. Elder, Carnegie Institution of Washington, Sept., 1939, pp. 1–27, MR **1**, 133.
70. Emma Lehmer, *Number Theory on the SWAC*, Proc. Sympos. Appl. Math., v. 6, Numerical Analysis, McGraw-Hill, 1956, 103–108, MR **18**, 74.
71. E. Lucas, *Théorie des Fonctions Numériques Simplement Periodiques*, Amer. J. Math. **1** (1878), 184–239; 289–321.
72. E. Lucas, *Théorie des Nombres,*Tome 1, Librarie Blanchard, Paris, 1961, MR **23** #A828.
73. Michael A. Morrison and John Brillhart, *The Factorization of F_7*, Bull. Amer. Math. Soc. **77** (1971), 264, MR **42** #3012.
74. Michael A. Morrison, *A Note on Primality Testing Using Lucas Sequences*, Math. Comp. **29** (1975), 181–182, MR **51** #5469.
75. Michael A. Morrison and John Brillhart, *A Method of Factoring and the Factorization of F_7*, Math Comp. **29** (1975), 183–205, MR **51** #8017.
76. C. Noll and L. Nickel, *The 25th and 26th Mersenne Primes*, Math. Comp. **35** (1980), 1387–1390, MR 81k:10010.
77. M. Penk (unpublished private communication).
78. P. Pépin, *Sur la Formule* $2^{2^n}+1$, C. R. Acad. Sci. Paris **85** (1877), 329–331.
79. H. C. Pocklington, *The Determination of the Prime or Composite Nature of Large Numbers by Fermat's Theorem*, Proc. Camb. Phil. Soc. **18** (1914-16), 29–30.
80. J. M. Pollard, *Theorems on Factorization and Primality Testing*, Proc. Camb. Phil. Soc. **76** (1974), 521–528, MR **50** #6992.
81. J. M. Pollard, *A Monte Carlo Method for Factorization*, BIT **15** (1975), No. 3, 331–335, MR **52** #13611.
82. Carl Pomerance, J. L. Selfridge and Samuel S. Wagstaff, Jr., *The Pseudoprimes to* $25\cdot10^9$, Math. Comp. **35** (1980), 1003–1026, MR 82g:10030.
83. P. Poulet, Sphinx **4** (1934), 175.
84. R. E. Powers, *Note on a Mersenne Number*, Bull. Amer. Math. Soc. **40** (1934), 883.
85. E. Proth, *Théorèmes sur les Nombres Premiers*, C. R. Acad. Sci. Paris **87** (1878), 926.
86. H. Riesel, *A New Mersenne Prime*, MTAC **12** (1958), 60.
87. H. Riesel, *Mersenne Numbers*, MTAC **12** (1958), 207–213, MR **21** #657.
88. H. Riesel, *A Factor of the Fermat Number F_{19}*, Math. Comp. **17** (1963), 458.
89. H. Riesel, *Some Factors of the Numbers $G_n=6^{2^n}+1$ and $H_n=10^{2^n}+1$*, Math. Comp. **23** (1969), 413–415, MR **39** #6813.
90. Raphael M. Robinson, *Mersenne and Fermat Numbers*, Proc. Amer. Math. Soc. **5** (1954), 842–846, MR **16**, 335.
91. Raphael M. Robinson, *Factors of Fermat Numbers*, MTAC **11** (1957), 21–22, MR **19**, 14.
92. Raphael M. Robinson, *Some Factorizations of Numbers of the Form $2^n\pm1$*, MTAC **11** (1957), 265–268, MR **20** #832.
93. Raphael M. Robinson, *The Converse of Fermat's Theorem*, Amer. Math. Monthly **64** (1957), 703–710, MR **20** #4520.
94. Raphael M. Robinson, *A Report on Primes of the Form $k.2^n+1$ and on Factors of Fermat Numbers*, Proc. Amer. Math. Soc. **9** (1958), 673–681, MR **20** #3097.
95. J. L. Selfridge, *Factors of Fermat Numbers*, MTAC **7** (1953), 274–275.
96. J. L. Selfridge and Alexander Hurwitz, *Fermat Numbers and Mersenne Numbers*, Math. Comp. **18** (1964), 146–148, MR **28** #2991.
97. J. L. Selfridge and Richard K. Guy, *Primality Testing with Applications to Small Machines*, Proc. Washington State Univ. Conf. on Number Theory, Pullman, 1971, pp. 45–51, MR **47** #8407.
98. J. L. Selfridge and M. C. Wunderlich, *An Efficient Algorithm for Testing Large Numbers for Primality*, Congressus Numerantium, v. 12, Proc. 4th Manitoba Conf. on Numerical Math., Winnipeg (1974), 109–120, MR **51** #5461.
99. Daniel Shanks, *Class Number, a Theory of Factorization, and Genera*, 1969 Number Theory Institute, Proc. Sympos Pure Math. **20**, Amer. Math. Soc., 1970, 415–440, MR **47** #4932.
100. D. E. Shippee, *Four New Factors of Fermat Numbers*, Math. Comp. **32** (1978), 941, MR **57** #12359.

101. David Slowinski, *Searching for the 27th Mersenne Prime*, J. Rec. Math. **11** (1978-79), 258–261, MR 80g:10013.
102. Bryant Tuckerman, *The 24th Mersenne Prime*, Proc. Nat. Acad. Sci. USA **68** (1971), 2319–2320, MR **45** #166.
103. Bryant Tuckerman, *A Search Procedure and Lower Bound for Odd Perfect Numbers*, Math. Comp. **27** (1973), 943–949, MR **48** #3853.
104. Bryant Tuckerman, *Odd-Perfect-Number Tree to* 10^{36}*, to Supplement 'A Search Procedure and Lower Bound for Odd Perfect Numbers'*, IBM Research Report RC4695, 1974. Copy deposited in the UMT file and reviewed in *Math. Comp.* **27** (1973), 1004–1005.
105. H. S. Uhler, *A New Result Concerning a Mersenne Number*, MTAC **1** (1943–45), 333, 404.
106. H. S. Uhler, *A Brief History of the Investigations of Mersenne's Numbers and the Latest Immense Primes*, Scripta Math. **18** (1952), 122–131, MR **14**, 343.
107. H. C. Williams, *A Generalization of Lehmer's Functions*, Acta Arith. **29** (1976), 315–341, MR **54** #220.
108. H. C. Williams and J. S. Judd, *Determination of the Primality of N by Using Factors of* $N^2 \pm 1$, Math. Comp. **30** (1976), 157–172, MR **53** #257.
109. H. C. Williams and J. S. Judd, *Some Algorithms for Prime Testing Using Generalized Lehmer Functions*, Math. Comp. **30** (1976), 867–886, MR **54** #2574.
110. H. C. Williams and R. Holte, *Some Observations on Primality Testing*, Math. Comp. **32** (1978), 905–917, MR **57** #16184.
111. H. C. Williams, *Primality Testing on a Computer*, Ars Combinatoria **5** (1978), 127–185, MR 80d:10002.
112. H. C. Williams, *Some Primes with Interesting Digit Patterns*, Math. Comp. **32** (1978), 1306–1310, MR **58** #484.
113. H. C. Williams and E. Seah, *Some Primes of the Form* $(a^n - 1)/(a - 1)$, Math. Comp. **33** (1979), 1337–1342, MR 80g:10014.
114. H. C. Williams and G. Matthew, *Some New Primes of the Form* $k.2^n + 1$, Math. Comp. **31** (1977), 797–798, MR **55** #12605.
115. Claude P. Wrathall, *New Factors of Fermat Numbers*, Math. Comp. **18** (1964), 324–325.
116. Marvin C. Wunderlich and J. L. Selfridge, *A Design for a Number theory Package with an Optimized Trial Division Routine*, Comm. ACM **17** (1974), 272–276.
117. C. R. Zarnke and H. C. Williams, *Computer Determination of Some Large Primes*, Congressus Numerantium, v. 3, Proc. of the Second Louisiana Conf. on Combinatorics, Graph Theory, and Computing, Utilitas Math., Winnipeg, 1971, 563–570.
118. H. Riesel, *En Bok Om Primtal*, Studentlitteratur, Lund, 1968, MR **42** #4507.

Additional references (201, 202, ...) for the second edition appear in section **IV B**. Additional references (301, 302, ...) for the third edition appear in section **V C**.