Perfect Numbers and Mersenne Primes

1986

Barry A. Delello

University of Central Florida

Find similar works at: https://stars.library.ucf.edu/rtd

University of Central Florida Libraries http://library.ucf.edu

Part of the Mathematics Commons

STARS Citation

https://stars.library.ucf.edu/rtd/4894

This Masters Thesis (Open Access) is brought to you for free and open access by STARS. It has been accepted for inclusion in Retrospective Theses and Dissertations by an authorized administrator of STARS. For more information, please contact lee.dotson@ucf.edu.
PERFECT NUMBERS AND MERSENNE PRIMES

BY

BARRY A. DELELLO
B.A., Syracuse University, 1976

THESIS

Submitted in partial fulfillment of the requirements for the Master of Science degree in Mathematics in the Graduate Studies Program of the College of Arts and Sciences University of Central Florida Orlando, Florida

Spring Term 1986
# TABLE OF CONTENTS

INTRODUCTION .................................................. 1

PART I. FOUNDATIONS: FROM EUCLID TO EULER ............... 3

PART II. FIBONACCI AND LUCAS .............................. 35

PART III. THE LUCAS-LEHMER THEOREM ....................... 42

PART IV. MODERN COMPUTER USAGE ........................... 61

  Horace Uhler and Charles B. Barker ...................... 62
  A. M. Turing ................................................. 63
  D. H. Lehmer and Raphael Robinson ....................... 64
  Hans Riesel .................................................. 65
  J. L. Selfridge and Alexander Hurwitz ................... 65
  Sidney Kravitz and Murray Berg ......................... 66
  Donald B. Gillies .......................................... 66
  Bryant Tuckerman ........................................... 68
  Laura Nickel and Curt Noll ............................... 69
  David Slowinski ............................................. 69
  Writing a Program .......................................... 71
  Description of the Program ................................ 72

APPENDIX A. ON ODD PERFECT NUMBERS ....................... 74

APPENDIX B. THE THIRTY KNOWN MERSENNE PRIMES .......... 76

APPENDIX C. COMPUTER PROGRAM ............................. 78

REFERENCES ..................................................... 87
INTRODUCTION

The intent of this paper is to present a history of the search for perfect numbers, from its first notable mention in Euclid's Elements to the current methodology using today's high-speed computers.

Despite the title, emphasis is placed on Mersenne primes. Since the topic of perfect numbers and Mersenne primes is so closely related (if you've found an example of one, then you've found an example of the other), it has been decided to include the latter in the title because of the overwhelming amount of information included on that topic. Current efforts towards finding perfect numbers make the topics practically indistinguishable.

The underlying theme behind this paper is two-fold. First, I wish to develop a theoretical structure which will support the various search methods employed over the centuries, as well as support a few other interesting results. Some parts of this structure lead to seemingly useless results; the fact that all even perfect numbers end in a 6 or a 28 is curious, and necessitates several supporting theorems, but the theorem is of little known use. On the other hand, the important Lucas-Lehmer Theorem, which greatly reduces the amount of computation required in the search, is the foundation of most, if not all, of today's efforts.
Secondly, I wish to explore the methods that are currently in use. Of major concern here are questions of storage of huge numbers, of efficiency of coding, and processor speed.

While one would normally expect a paper on a mathematical topic to be overflowing in symbolism, epsilons, deltas and the like, the proper coverage of this topic is impossible without considering the historical context. An effort has been made to develop the theory in relationship to its historical development. This sometimes leads to situations where the theorems are reversed from the order in which they are traditionally taught today.

It is assumed that the reader of this paper has had at least one course in number theory. Every effort has been made, however, to keep the mathematics at an elementary level, requiring the reader to assume very little that falls predominantly in the realm of the theory of numbers. Of course, the paper relies heavily on the properties of the positive integers. It also sets well on the basic, easily provable properties of congruences. The only other topic which is used without much discussion concerns Euler's $\phi$-function.
The history of mathematics is replete with unanswered questions and numerous well-researched, yet still unproven conjectures. Perhaps no other branch of mathematics has more than its share of puzzles than the theory of numbers. The theory of numbers and its numerous unsolved problems has attracted the attention of mathematicians, both amateur and professional alike, since the time of the Pythagoreans.

Shanks writes, "Much of elementary number theory arose out of the investigation of three problems; that of perfect numbers, that of periodic decimals, and that of Pythagorean numbers." (Shanks 1978) Perhaps one of the greatest contributors to the theory of numbers was French mathematician Pierre de Fermat who, while answering to the challenges of Frenicle and Mersenne concerning perfect numbers, developed two important theorems and a class of numbers, all of which bear his name.

DEFINITION 1. A positive integer \( n \) is said to be perfect if \( n \) is equal to the sum of all its positive divisors other than itself.

The first perfect number is 6, i.e.,

\[ 6 = 1 + 2 + 3 \]
Similarly,

\[
28 = 1 + 2 + 4 + 7 + 14 \\
496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 \\
8128 = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + \\
+ 1016 + 2032 + 4064
\]

and so on.

Some authors tend to favor the use of the number-theoretic function \( \sigma(n) = \sum d \), the sum of the positive integral divisors of \( n \), thus we can reword Definition 1 to read:

**DEFINITION 1 (alternate).** A positive integer \( n \) is said to be perfect if \( \sigma(n) = 2n \).

The origin of the study of perfect numbers is lost to antiquity. Supernatural powers and mythical meanings were often ascribed to many numbers during the pre-Christian era, and perfect numbers were often used to explain natural, physical and theological phenomena.

The first known analytical treatment of the subject of which we still have evidence was attributed to the Greek mathematician Euclid (fl. 300 B.C.) in Book IX of his *Elements*. *Elements* has a universal reputation as a book on geometry, but Euclid included much information on the theory of numbers as well.

Euclid's great contribution to the study of perfect numbers was his observation of the forms of the even perfect numbers. Euclid proved that if \( p = 1 + 2 + 2^2 + 2^3 + \ldots + 2^n \) is a prime, then \( 2^{n-1}p \) is a perfect
number. The following is a translation of Euclid's theorem. The
numbers in brackets at the end of some lines refer to previous theorems
in Euclid's work; hence, "VII. 14" refers to Book VII, Proposition 14.

PROPOSITION 36.
If as many numbers as we please beginning from an unit be set out
continuously in double proportion, until the sum of all becomes
prime, and if the sum multiplied into the last make some number,
the product will be perfect.

For let as many numbers as we please, A, B, C, D, beginning
from an unit be set out in double proportion, until the sum of
all becomes prime. Let E be equal to the sum, and let E by mul-
tiplying D make FG; I say that FG is perfect.

For, however many A, B, C, D are in multitude, let so many
E, HK, L, M be taken in double proportion beginning from E;
therefore, ex aequali, as A is to D, so is E to M. [VII. 14]

Therefore the product of E, D is equal to the product of
A, M. [VII. 19]

And the product of E, D is FG; therefore the product of
A, M is also FG. Therefore A by multiplying M has made FG; there-
fore M measures FG according to the units in A. And A is a dyad;
therefore FG is double of M.

But M, L, HK, E are continuously double of each other;
therefore E, HK, L, M, FG are continuously proportional in double
proportion.
Now let there be subtracted from the second HK and the last FG the numbers HN, FO, each equal to the first E; therefore, as the excess of the second is to the first, so is the excess of the last to all those before it. [IX. 35]

Therefore, as NK is to E, so is OG to M, L, KH, E. And NK is equal to E; therefore OG is also equal to M, L, HK, E. But FO is also equal to E, and E is equal to A, B, C, D, and the unit.

Therefore the whole FG is equal to E, HK, L, M and A, B, C, D and the unit; and is measured by them.

I say also that FG will not be measured by any other number except A, B, C, E, HK, L, M and the unit. For, if possible, let some other number P measure FG, and let P not be the same with any of the numbers A, B, C, D, E, HK, L, M. And, as many times as P measures FG, so many units let there be in Q; therefore Q by multiplying P has made FG.

But, further, E has also by multiplying D made FG; therefore, as E is to Q, so is P to D. [VII. 19]

And, since A, B, C, D are continuously proportional beginning from an unit, therefore D will not be measured by any other number except A, B, C. [IX. 13]

And, by hypothesis, P is not the same with any of the numbers A, B, C; therefore P will not measure D. But, as P is to D, so is E to Q; therefore neither does E measure Q. [VII. Def. 20]

And E is prime: and any prime number is prime to any number which it does not measure. [VII. 21]

Therefore E, Q are prime to one another. But primes are also least, [VII. 29] and the least numbers measure those which have the same ratio the same number of times, the antecedent the antecedent and the consequent the consequent; [VII. 20] and, as E is to Q, so is P to D; therefore E measures P the same number of times that Q measures D.

But D is not measured by any other number except A, B, C; therefore Q is the same with one of the numbers A, B, C. Let it be the same with B. And, however many B, C, D are in multitude, let so many E, HK, L be taken beginning from E.

Now E, HK, L are in the same ratio with B, C, D; therefore, ex aequali, as B is to D, so is E to L. [VII. 14]
Therefore the product of B, L is equal to the product of D, E.\[\text{[VII. 19]}\]

But the product of D, E is equal to the product of Q, P; therefore the product of Q, P is also equal to the product of B, L. Therefore, as Q is to B, so is L to P.\[\text{[VII. 19]}\]

And Q is the same with B; therefore L is also the same with P; which is impossible, for by hypothesis P is not the same with any of the numbers set out.

Therefore no number will measure FG except A, B, C, D, E, HK, L, M and the unit. And FG was proved equal to A, B, C, D, E, HK, L, M and the unit; and a perfect number is that which is equal to its own parts; therefore FG is perfect (Heath, 1956).\[\text{[VII. Def. 22]}\]

The editor (Heath) of this reference gives the following translation, recognizing the inherent difficulty the modern reader might have with Euclid's prose:

If the sum of any number of terms of the series

\[1, 2, 2^2, \ldots, 2^{n-1}\]

be prime, and the said sum be multiplied by the last term, the product will be a perfect number, i.e., equal to the sum of all its factors.

Let \(1 + 2 + 2^2 + \ldots + 2^{n-1} (= s_n)\) be prime; then shall

\[s_n \cdot 2^{n-1}\]

be "perfect."

Take \((n-1)\) terms of the series

\[s_n, 2s_n, 2^2s_n, \ldots, 2^{n-1}.

Therefore, \text{ex aequali},

\[2 : 2^{n-1} = s_n : 2^{n-2}s_n,\] \[\text{[VII. 14]}\]

or \[2 \cdot 2^{n-2}s_n = 2^{n-1}s_n.\] \[\text{[VII. 19]}\]

(This is, of course, obviously algebraically, but Euclid's notation requires him to prove it.)

Now, by IX. 35, we can sum the series

\[s_n + 2s_n + \ldots + 2^{n-2}s_n,\] and
\[(2S_n - S_n) : S_n = (2^{n-1}S_n - S_n) : (S_n + 2S_n + \ldots + 2^{n-2}S_n).\]

Therefore,
\[S_n + 2S_n + 2^2S_n + \ldots + 2^{n-2}S_n = 2^{n-1}S_n - S_n,\]
or
\[2^{n-1}S_n = S_n + 2S_n + 2^2S_n + \ldots + 2^{n-2}S_n + S_n\]
\[= S_n + 2S_n + \ldots + 2^{n-2}S_n + (1 + 2 + 2^2 + \ldots + 2^{n-1}),\]
and \(2^{n-1}S_n\) is measured by every term of the right hand expression.

It is now necessary to prove that \(2^{n-1}S_n\) cannot have any factor except those terms.

Suppose, if possible, that it has a factor \(x\) different from all of them, and let \(2^{n-1}S_n = x \cdot m.\)

Therefore,
\[S_n : m = x : 2^{n-1}\]  \[\text{[VII. 19]}\]

Now \(2^{n-1}\) can only be measured by the preceding terms of the series \(1, 2, 2^2, \ldots, 2^{n-1}\), \[\text{[IX. 13]}\] and \(x\) is different from all of these; therefore \(x\) does not measure \(2^{n-1}\), so that \(S_n\) does not measure \(m.\) \[\text{[VII. Def. 20]}\]

And \(S_n\) is prime; therefore it is prime to \(m.\) \[\text{[VII. 29]}\]

It follows from [VII. 20, 21] that \(m\) measures \(2^{n-1}\).

Suppose that \(m = 2^r\). Now, \(\text{ex aequali},\)
\[2^r \cdot 2^{n-r-1}S_n = 2^{n-1}S_n\]  \[\text{[VII. 19]}\]
\[= x \cdot m,\] from above.

And \(m = 2^r\); therefore \(x = 2^{n-r-1}S_n\), one of the terms of the series \(S_n, 2S_n, 2^2S_n, \ldots, 2^{n-2}S_n, 1, 2, 2^2, \ldots, 2^{n-1}\); which contradicts the hypothesis.

Therefore \(2^{n-1}S_n\) has no factors except
\[S_n, 2S_n, 2^2S_n, \ldots, 2^{n-2}S_n, 1, 2, 2^2, \ldots, 2^{n-1}.\]

(Heath 1957)
Euclid's theorem formed the foundation of perfect number searches for over two thousand years (roughly from 300 B.C. to the late 19th Century.) Many scholars in Medieval and Renaissance times were under the impression that Euclid's method generated perfect numbers in general, and often announced several "perfect numbers" of higher magnitude that were generated by Euclid's method, even though they had no reasonable proof of the implied primality. As will be pointed out in the mid-20th Century, the perfect numbers generated by this method are actually quite sparse. Other misconceptions included the belief that Euclid's theorem established all perfect numbers (as of yet unproven) that the perfect numbers of Euclid's type alternately end in a 6 or an 8 (refuted by the 15th Century), and that the \( n \)th perfect number contains \( n \) digits (there is no perfect number of five digits). The best reference on the early research on perfect numbers remains Chapter I of L. E. Dickson's Theory of Numbers (Dickson 1971).

Following are two examples of a more modern approach to proving Euclid's theorem. The first is a quick and simple proof making use of the \( \sigma(n) \) function. While making several assumptions about existence and uniqueness of representation, it basically outlines the more rigorous treatment that follows.

**Theorem 1.** An even integer is a perfect number if it is of the form

\[
2^{p-1}(2^p - 1)
\]

where \( 2^p - 1 \) is a prime.

**Proof (Pettofrezzo):** Let \( n = 2^{p-1}(2^p - 1) \) where \( 2^p - 1 \) is prime.

Then,
\[
\sigma(n) = (1 + 2 + 2^2 + \ldots + 2^{P-1})[1 + (2^P - 1)]
\]
\[
= \frac{2^P - 1}{2 - 1} \cdot 2^P
\]
\[
= 2^P(2^P - 1)
\]
\[
= 2n.
\]

Now, for a more rigorous approach. As is any mathematical proof, one must make a decision about what to prove and what to accept as self-evident. It is the intention of the author to write this paper based solely on fundamental ideas of the theory of numbers, leaving little to be questioned. Thus, the following treatment of Euclid's theorem is first supported by some foundation lemmas.

**Lemma 1. The Division Algorithm.** Given integers \(a\) and \(b\), with \(a > 0\), there exist unique integers \(q\) and \(r\) such that \(b = qa + r\), \(0 \leq r < a\). If \(a\nmid b\), then \(r\) satisfies the stronger inequalities \(0 < r < a\).

**Proof (Niven and Zuckerman 1972):** Consider the arithmetic progression
\[
\ldots, b - 3a, b - 2a, b - a, b + a, b + 2a, \ldots
\]
extending indefinitely in both directions. In this sequence, select the smallest non-negative member and denote it by \(r\). Thus, by definition \(r\) satisfies the inequalities of the theorem. But also \(r\), being in the sequence, is of the form \(b - qa\), and thus \(q\) is defined in terms of \(r\).

To prove the uniqueness of \(q\) and \(r\), suppose there is another pair \(q_1\) and \(r_1\) satisfying the same conditions. First we prove that \(r_1 = r\). For if not, we may presume that \(r < r_1 < r < a\)
and then we see that \( r_1 - r = a(q - q_1) \) and so \( a|\( r_1 - r \) \), a contradiction to a basic property of divisibility (i.e., \( a|b \), \( a > 0 \), \( b > 0 \), imply \( a \leq b \)). Hence \( r = r_1 \) and \( q = q_1 \).

**Lemma 2.** The Euclidean Algorithm (Euclid). If \( g = (a, b) \) (i.e., the greatest common divisor of \( a \) and \( b \)) there is a linear combination of \( a \) and \( b \) with integral coefficients \( m \) and \( n \) (positive, negative or zero) such that

\[
g = ma + nb.
\]

**Proof:** Without loss of generality, let \( a \leq b \) and divide \( b \) by \( a \):

\[
b = q_0 + a_1
\]

with a positive quotient \( q_0 \) and a remainder \( a_1 \) where

\[
0 < a_1 < a.
\]

Existence is guaranteed by Lemma 1. If \( a_1 \neq 0 \), divide \( a \) by \( a_1 \) and continue the process until some remainder, \( a_{n+1} \), equals 0.

\[
a = q_1a_1 + a_2
\]

\[
a_1 = q_2a_2 + a_3
\]

\[
\vdots
\]

\[
a_{n-2} = q_{n-1}a_{n-1} + a_n
\]

\[
a_{n-1} = q_na_n.
\]

This must occur, since \( a > a_1 > a_2 > \ldots > 0 \).

Now, from the first equation, (1), since \( g|a \) and \( g|b \), we have \( g|a_1 \). Then, from the second equation, since \( g|a \) and \( g|a_1 \) we have \( g|a_2 \). By induction, \( g|a_n \), and therefore

\[
g \leq a_n.
\]
But, conversely, since \( a_n \mid a_{n-1} \) by the last equation, by working backwards through the equations we find that \( a_n \mid a_{n-2}, a_n \mid a_{n-3}, \ldots, a_n \mid a \) and \( a_n \mid b \). Thus \( a_n \) is a common divisor of \( a \) and \( b \) and

\[
a_n \leq g \text{ (the greatest)}.
\]

With equation (2), we therefore conclude that \( g = a_n \).

Now, from the next-to-the-last equation, \( a_n \) is a linear combination, with integral coefficients, of \( a_{n-1} \) and \( a_{n-2} \). Again, working backwards we see that \( a_n \) is a linear combination of \( a_{n-1} \) and \( a_{n-1-1} \) for every \( i \).

Finally,

\[
g = a_n = ma + nb
\]

for some integers \( m \) and \( n \).

Note: Lemma 5 is a corollary.

**Lemma 3** (Euclid). If \( a, b, \) and \( c \) are integers such that

\[
c \mid ab \text{ and } (c, a) = 1,
\]

then \( c \mid b \).

**Proof:** By Lemma 2,

\[
mc + na = 1.
\]

Therefore,

\[
mcb + nab = b,
\]

but since \( c \mid ab, ab = cd \) for some integer \( d \). Thus,

\[
c(mb + nd) = b,
\]

or \( c \mid b \).
COROLLARY TO LEMMA 3. If a prime \( p \) divides a product of \( n \) numbers, i.e.,
\[ p \mid a_1 a_2 a_3 \ldots a_n, \]
it must divide at least one of them.

PROOF: If \( p \nmid a_1 \), then \((a_1, p) = 1\). If now, \( p \nmid a_2 \), then we must have \( p \nmid a_1 a_2 \), for by Lemma 3, if \( p \mid a_1 a_2 \), then \( p \mid a_2 \). It follows that if \( p \nmid a_1, p \nmid a_2 \) and \( p \nmid a_3 \), then \( p \nmid a_1 a_2 a_3 \). By induction, if \( p \) divided none of the \( a_i \)'s, then it could not divide their product. Thus, the contrapositive of this last statement, our corollary, must also be true.

LEMMA 4. THE FUNDAMENTAL THEOREM OF ARITHMETIC. Every integer \( N > 1 \) has a unique factorization into primes, \( p_i \), in a standard form,
\[ N = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}, \tag{3} \]
with \( a_1 > 0 \) and \( p_1 < p_2 < \ldots < p_n \). That is, if
\[ N = q_1^{b_1} q_2^{b_2} \ldots q_m^{b_m}, \tag{4} \]
for primes \( q_1 < q_2 < \ldots < q_m \) and exponents \( b_i > 0 \), then \( p_i = q_i \), \( m = n \), and \( a_i = b_i \).

PROOF (Shanks 1978): First, \( N \) must have at least one representation, equation (3). Let \( a \) be the smallest divisor of \( N \) which is \( > 1 \). It must be a prime, since if not, \( a \) would have a divisor \( > 1 \) and \( < a \). This divisor, \( < a \), would divide \( N \) and this contradicts the definition of \( a \). Now write \( a \) as \( p_1 \), and the quotient \( N/p_1 \) as \( N_1 \). Repeat the process with \( N_1 \). The process must terminate, since
\[ N > N_1 > N_2 > \ldots > 1. \]
This generates equation (3). Now, if there were a second representation, by the Corollary to Lemma 3, each $p_i$ must equal some $q_i$, since $p_i|N$. Likewise, each $q_i$ must divide some $p_i$. Therefore $p_i = q_i$ and $m = n$. If $b_i > a_i$, divide $p_i^{a_i}$ into equations (3) and (4). Then $p_i$ would divide the quotient in equation (4) but not in equation (3). This contradiction shows that $a_i = b_i$.

**COROLLARY TO LEMMA 4.** The only positive divisors of

$$N = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$$

are those of the form

$$p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}$$

where

$$0 \leq c_i \leq a_i.$$  

**PROOF** (Shanks 1978): Let $f|N$ and write $N = fg$. Express $f$ and $g$ in the standard form. Then if $f$ and $g$ were not both in the form of equation (5), their product, $N$, would have a representation distinct from equation (3). This contradiction proves the corollary.

**THEOREM 1** (again). The number $2^{P-1}(2^P-1)$ is perfect if $2^P-1$ is a prime.

**Note:** Before we continue, the sharp eye might have noticed that his reformulation of Theorem 1 has actually changed its
statement. Here we are saying that any number of the form $2^{P-1}(2^P-1)$ is perfect if $2^P-1$ is prime, while in the original treatment we made the stronger statement that all even perfect numbers are necessarily of this form. We will treat the exact reformulation of the original Theorem 1 as Theorem 4.

PROOF: Let $N = 2^{P-1}(2^P-1)$ where $2^P-1$ is a prime. The only positive divisors of $2^{P-1}(2^P-1)$ are

1 and $(2^P-1)$
2 and $2(2^P-1)$
$2^2$ and $2^2(2^P-1)$

...  
$2^{P-1}$ and $2^{P-1}(2^P-1)$.

Thus, $\sigma(n)$, the sum of these divisors, including the last, is equal to

$$\sigma(n) = 1 + 2 + 2^2 + \ldots + 2^{P-1} + (2^P-1) + 2(2^P-1) +$$
$$+ 2^2(2^P-1) + \ldots + 2^{P-1}(2^P-1)$$
$$= (1 + 2 + 2^2 + \ldots + 2^{P-1})(1 + (2^P-1))$$
$$= (2^P-1)(2^P)$$
$$= 2N.$$ 

Therefore, the sum of this set of divisors, mentioned above, excluding $N$ itself, is

$$\sigma(n) - N = N.$$

Thus, $N$ is perfect.

How do we know that $N$ doesn't have other divisors? The Corollary to Lemma 4 assures us that there are not.
The remainder of this section deals with the progress in the methods for finding perfect numbers from Euclid's time to about the late 18th Century.

The only perfect numbers known to the Greeks were the four previously mentioned; 6, 28, 496 and 8128. Research of that time was wrought with false assumptions and erroneous conjectures. Numerous conjectures of that era remain unsolved to this day. No one has yet to find an odd perfect number or prove that they do not exist. Whether or not there is an infinite number of perfect numbers of Euclid's type or otherwise also remains unanswered.

The first few hundred years of the Christian era produced nothing new about perfect numbers. The subject was occasionally mentioned in manuscripts dating back to that time, but nothing new was evidently published. Then in the 15th Century an unknown author penned a list of perfect numbers in the manuscript "Codex lat. Monac. 14908, a part dated 1456 and a part 1461." (Dickson 1971) Unlike previous authors who traditionally believed that $2^9 - 1$ and $2^{11} - 1$ were prime, this author correctly called the fifth perfect number 33,550,336 (corresponding to $2^{12}(2^{13} - 1)$). What seems difficult to believe by the modern reader was that few Medieval writers bothered to check the few minutes of easy arithmetic that it would require to show that $2^9 - 1 = 7 \cdot 73$ or that $2^{11} - 1 = 23 \cdot 89$. One possible explanation is that the Middle Ages were really a dormant period for scientific thought in Europe and that nobody really cared, except for the centers of learning of that time, the monasteries. Another possible reason is that may have been that a lot of the texts that we
have knowledge of were actually the work of scribes rather than the original authors, and it is likely that misconceptions could be handed down for centuries by people who were more concerned with appearance than with content.

The Italian mathematician Pietro Cataldi (1548-1626) was the first to clear up several misconceptions concerning perfect numbers. His treatise Trattato de numeri perfetti di Pietro Antonio Cataldo must have been a monumental work at the time, noting the several theorems that he developed and the myths that he debunked. (The work was published in Bologna in 1603, but his preface states that it was actually written in 1588.) Cataldi verified that the Medieval \(2^{13} - 1\) was indeed a prime, and that \(2^{17} - 1 = 131,071\) was also a prime, thus making \(2^{16}(2^{17} - 1)\) the sixth perfect number. His method was the best known to him at the time, ... divide the suspect number by every prime less than the square root of the number (Dickson 1971). That would require 24 and 72 divisions respectively.

Not succumbing to writer's cramp, Cataldi also performed the 128 divisions necessary to show that \(2^{19} - 1\) was also a prime. The year was 1588. The next perfect number of Euclid's type, \(2^{30}(2^{31} - 1)\) would require 4,792 divisions by Cataldi's method (Shanks 1978), thus leaving it somewhat out of his reach.

Cataldi also showed that if \(2^p - 1\) is to be prime, then \(p\) must be prime (Theorem 2). This finally shed some light on the mistaken belief that the sequence generated by \(2^p - 1(2^p - 1)\), \(p = 2, 3, 4, \ldots\) generated perfect numbers, in general, although word was slow to
travel around 17th Century Europe. This also makes Cataldi the father of Mersenne primes, although he did not get the honor. Cataldi was quick to point out that the converse of the above statement was certainly false, as 11 is a prime and $2^{11} - 1$ was well known to be composite.

**THEOREM 2** (Cataldi, Fermat). If $a^k - 1$ is prime ($a > 0, k \geq 2$), then $a = 2$ and $k$ is also a prime.

**PROOF:** It can easily be shown, by performing the actual division, that

$$a^k - 1 = (a - 1)(a^{k-1} + a^{k-2} + \ldots + a + 1) \quad (6)$$

Since $a^{k-1} + a^{k-2} + \ldots + a + a \geq a + 1 \geq 1$, and since $a^k - 1$ is prime in equation (6), its factor of $(a - 1)$ must equal 1, or $a = 2$.

If $k$ is not prime, denote it as $k = rs$, with $r > 1$ and $s > 1$. Then

$$2^k - 1 = 2^{rs} - 1 = (2^r)^s - 1$$

$$= (2^r(s-1) + 2^r(s-2) + \ldots + 2^r + 1) \cdot (2^r - 1).$$

Each term on the right is clearly greater than 1, thus $2^k - 1$ is composite, a contradiction. Thus $k$ is also prime.

Cataldi's work, mentioned previously, was also noted as being the source of the first extensive list of prime numbers. Dickson (1971) wrote "He gave a table of all divisors of all even and odd numbers $\leq 800$, and a table of primes $\leq 750."$ Note that $724 \sqrt{2^{19}} - 1$
< 725. He also appears to be the first to publish a proof that, while perfect numbers do not necessarily alternately end with a 6 or an 8, \( P_5 = 33,550,336 \) and \( P_6 = 8,589,869,056 \), they do necessarily end in a 6 or an 8 (Theorem 3).

**THEOREM 3** (Cataldi). Every perfect number of Euclid's type ends in a 6 or an 8.

(Note: Euler later showed that all even perfect numbers are necessarily of Euclid's type.)

**PROOF:** Let \( N \) be an even perfect number of Euclid's type:

\[
N = 2^{p-1}(2^p - 1)
\]

where \( p \) is necessarily a prime (by Theorem 2).

Every prime \( > 2 \) is of the form \( 4m + 1 \) or \( 4m + 3 \), otherwise it would be divisible by 2. Let \( p \) be of the form \( 4m + 1 \). Then,

\[
N = 2^{4m}(2^{4m+1} - 1)
= 16^m(2 \cdot 16^m - 1) \text{ with } m \geq 1.
\]

But, ... by induction, it is clear that \( 16^m \) always ends in a 6. Therefore, \( 2 \cdot 16^m - 1 \) always ends in a 1, and \( N \) always ends in a 6. Similarly, let \( p \) be of the form \( 4m + 3 \). Then,

\[
n = 2^{4m+2}(2^{4m+3} - 1)
= 4 \cdot 16^m(8 \cdot 16^m - 1) \text{ with } m \geq 1.
\]

Thus, \( 4 \cdot 16^m \) ends in a 4, while \( 8 \cdot 16^m - 1 \) ends in a 7. Therefore, \( N \) ends in an 8.
Finally, if \( p = 2 \), we have \( N = P_1 = 6 \), proving that all perfect numbers of Euclid's type end in a 6 or an 8.

Actually, this theorem can be a bit more restrictive, ...

**COROLLARY TO THEOREM 3.** Every perfect number of Euclid's type ends in a 6 or a 28.

**PROOF:** We need to show that primes of the form \( 4m + 3 \) generate perfect numbers that end in 28. Let \( p \) be of that form.

Then,

\[
2^{p-1} = 2^{(4m+3)-1} = 2^{4m+2} = 2^m2^2 = 16^m.4.
\]

Thus,

\[
2^{p-1} \equiv 4 \pmod{10}.
\]

Since, in our application, \( p \geq 3 \), then \( 2^{p-1} \geq 2^2 \), and \( 4|2^{p-1} \). So, \( \ldots \) \( 2^{p-1} \) is divisible by 4 and also ends in a 4.

Equivalently, we can say that

\[
2^{p-1} \equiv 4, 24, 44, 64, \text{ or } 84 \pmod{100}
\]

Thus, for those six cases, we can see that

\[
2 \cdot 2^{p-1} - 1 \equiv 7, 47, 87, 27, \text{ or } 67 \pmod{100},
\]

respectively.

Therefore, if \( 2^{p-1} = 4 \pmod{100} \), then \( 2^p - 1 \equiv 7 \pmod{100} \), and \( 2^{p-1}(2^p - 1) = 28 \pmod{100} \); if \( 2^{p-1} = 24 \pmod{100} \), then \( 2^p - 1 = 47 \pmod{100} \), and \( 2^{p-1}(2^p - 1) = 1128 \pmod{100} = 28 \pmod{100} \). The other three cases follow suit, being congruent to 3828, 1728 and 5628 \pmod{100} respectively, all congruent to 28.
Cataldi still believed that $2^{P-1}(2^P - 1)$, with $p$ a prime, generated perfect numbers, in general, and so stated that $2^P - 1$ was prime for $p = 2$, $3$, $5$, $7$, $13$, $17$, $19$, $23$, $29$, $31$, and $37$. The defiance of $p = 11$, he evidently felt, was not compelling.

Skipping ahead over a century (for only a moment), Swiss mathematician Leonhard Euler (1707-1783) eventually proved that all even perfect numbers are necessarily of Euclid's type. His proof was remarkably simple ...

**THEOREM 4** (Euler). Every even perfect number is of the form $2^{P-1}(2^P - 1)$, $2^P - 1$ a prime.

Note: See original Theorem 1 for a concise version.

**PROOF** (L.E. Dickson, (Shanks 1978)): Let $N$ be an even perfect number given by

$$N = 2^{P-1}F$$

where $F$ is an odd number.

Let $\sigma(F)$ be the sum of the positive divisors of $F$. The positive divisors of $N$ include all these odd divisors and their doubles, their multiples of 4, ..., their multiples of $2^{P-1}$. There are no other positive divisors (by the Corollary to Lemma 4).

Since $N$ is perfect we have:

$$N = 2^{P-1}F = (1 + 2 + \ldots + 2^{P-1}) \sigma(F) - N$$

or

$$2N = 2^PF = (2^P - 1) \sigma(F).$$

Therefore,

$$\sigma(F)(2^P - 1) = 2^PF - F + F = F(2^P - 1) + F$$
or \( \sigma(F) = F + F/(2^p - 1) \). \( (7) \)

and since \( \sigma(F) \) and \( F \) are integers, so must \( F/(2^p - 1) \) be an integer. Thus,

\[ (2^p - 1)|F \]

and \( F/(2^p - 1) \) must be one of the divisors of \( F \). Since \( \sigma(F) \) is the sum of all the positive divisors of \( F \), we see from equation (7) that there can be only two, namely \( F \) itself and \( F/(2^p - 1) \). But 1 is certainly a divisor of \( F \). Since \( F \) cannot equal 1, we must have \( F/(2^p - 1) = 1 \), or \( F = 2^p - 1 \), a prime.

Modern custom refers to numbers of the form \( 2^p - 1 \), \( p \) prime, with the abbreviation

\[ M_p = 2^p - 1, \]

henceforth called Mersenne numbers. Should \( M_p \) be prime, the name Mersenne prime applies. The nomenclature is after a French monk named Marin Mersenne (1588-1648) who popularized number theory research in the early 17th Century. While not an outstanding mathematician in his own right, Mersenne counted Descartes and Fermat among his friends and delighted in posing challenging questions in correspondence to the two.

Who was Marin Mersenne? Uhler (1952) writes,

He was born near Oize (Sarthe) on Sept. 8, 1588, and died in Paris on Sept. 1, 1648. Mersenne and Descartes were fellow students at the Jesuit college of La Flèche. In 1611 Mersenne joined the Minim Friars, and in 1620 he made a permanent residence in Paris at the convent of L'Annonciade.
Mersenne was most noted for making the assertion, in his *Cogita Physica-Mathematica* (1644), that the first 11 perfect numbers belonged to the primes 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 and 257 (Burton 1976). It wasn't until 1947 that this assertion was exhaustively analyzed. As it was, Mersenne missed \( p = 61 \), 89 and 107 while \( p = 67 \) and \( p = 257 \) proved to be composite. Some supporters of Mersenne have concluded that his inclusion of \( p = 67 \) instead of \( p = 61 \) was probably a slip of the pen on somebody's part.

It was in a letter to Mersenne that Fermat first announced his discovery, among many others, that \( 2^P - 1 \) is divisible only by primes of the form \( 2kp + 1 \) (Theorem 5). Theorem 5 needs two additional supporting lemmas:

**Lemma 5** Let \( k \) be the smallest positive integer such that \( 2^t \equiv 1 \pmod{q} \). Then for any positive integer \( p \) such that \( 2^P \equiv 1 \pmod{q} \), we must have \( k|p \).

**Proof:** Let \( p \) be any positive integer such that \( 2^p \equiv 1 \pmod{q} \). By the Division Algorithm (Lemma 1), there exists unique integers \( s \) and \( r \) such that \( p = sk + r \), where \( 0 \leq r < k \). Thus,

\[
2^p = 2^{sk+r} = (2^k)^s 2^r.
\]

Since \( 2^p \equiv 1 \pmod{q} \) and \( 2^k \equiv 1 \pmod{q} \), we can conclude that \( 2^r \equiv 1 \pmod{q} \). Since \( 0 \leq r \leq k \), we have a situation where \( k \) is no longer the smallest positive integer such that \( 2^t \equiv 1 \pmod{q} \), a contradiction. Thus \( r = 0 \) and \( p = sk \), or \( k|p \).
LEMMA 6. FERMAT'S LITTLE THEOREM. For every prime p and every integer a such that p|a,

\[ p | a^{p-1} - 1 \text{ (i.e., } a^{p-1} \equiv 1 \pmod{p} \). \]

PROOF: The numbers a, 2a, 3a, ..., (p-1)a are congruent (mod p) in some order to 1, 2, 3, ..., p-1, being as it is, a complete residue system.

Thus,

\[ a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (p-1) \pmod{p} \]

or \[ a^{p-1}(p-1)! \equiv (p-1)! \pmod{p} \]

or \[ p | a^{p-1}(p-1)! - (p-1)! \]

or \[ p | (p-1)!(a^{p-1} - 1). \]

However, \((p,(p-1)!)\) is clearly equal to 1.

Therefore,

\[ p | a^{p-1} - 1, \text{ by Lemma 3,} \]

or \[ a^{p-1} \equiv 1 \pmod{p}. \]

COROLLARY TO LEMMA 6. If p is a prime, then \[ a^p \equiv a \pmod{p} \] for any integer a.

PROOF: If p|a, then the situation is trivial; for by induction, p would divide \[ a^k, \ k > 1, \] giving us \( p | a^k - a \) or \[ a^k \equiv a \pmod{p} \). If p \( \not| a \), then we can rely on the Lemma, for if \[ a^{p-1} \equiv 1 \pmod{p}, \]

then by multiplying both sides of the congruence by a, we get \[ a^p \equiv a \pmod{p}. \]
Euler later generalized Fermat's Little Theorem with the following result:

If \((a,m) = 1\) then \(a^{\phi(m)} \equiv 1 \pmod{m}\),

where \(\phi(m)\), called Euler's \(\phi\)-function is defined to be the number of positive integers less than or equal to \(m\) that are relatively prime to \(m\).

Euler's theorem has proven so popular that most number theory text writers prefer to introduce it first and include Fermat's work as a special case. A few of the theorems in this paper can be made much easier by the known properties of the \(\phi\)-function, however in my determination to keep this paper in historical perspective, admitting the \(\phi\)-function would, as it may, be putting the cart before the horse.

**THEOREM 5** (Fermat, 1640). If \(p\) is an odd prime, any prime which divides \(M_p\) must be of the form \(2kp + 1\), with \(k = 1, 2, 3, 4, ...\).

**Proof:** Let \(q|M_p\), i.e., \(q|2^p - 1\) or \(2^p \equiv 1 \pmod{q}\).

Let the positive integer \(k\) be the smallest such \(p\). Then, by Lemma 5, we know \(k|p\).

Obviously, \(k \neq 1\), as \(q|2^k - 1 \Rightarrow q|1\), a contradiction as \(q\) is prime.

Thus, since \(k|p\), \(k > 1\) implies \(k = p\).

By Fermat's Little Theorem, \(q|2^{q-1} - 1\), or \(2^{q-1} \equiv 1 \pmod{q}\). Note again that \(k|q-1\) by Lemma 5. Since \(p = k\), then \(p|q-1\) or \(pt = q-1\), which implies that \(pt + 1 = q\) for some \(t\). Note however that \(t\), odd implies \(pt\), odd implies \(q\), even, a contradiction, since \(q|2^p - 1\) implies \(q\) is odd.
Thus, any prime which divides \( M_p \) must be of the form \( kp + 1, \ k = 2, 4, 6, 8, \ldots \), or equivalently, of the form \( 2kp + 1, \ k = 1, 2, 3, 4, \ldots \).

Euler later proved a similar theorem, that every divisor of \( M_p \) is of the form \( 8k \pm 1 \), theoretically of much practical use when used concurrently with Theorem 5. However, Euler's result (Theorem 6) requires much more involved concepts of number theory, described herein as Lemmas 7 through 10.

**DEFINITION:** \( n \) is a **quadratic residue** modulo \( m \) if \( x^2 \equiv n \pmod{m} \) is solvable. Otherwise, \( n \) is a quadratic non-residue modulo \( m \). In either case we assume that \( (n,m) = 1 \).

**DEFINITION:** If \( p \) is an odd prime and \( (a,p) = 1 \), then we define the Legendre symbol \( \left( \frac{a}{p} \right) \) to be 1 if \( a \) is a quadratic residue \( \pmod{p} \) and to be -1 if \( a \) is a quadratic non-residue \( \pmod{p} \).

**LEMMA 7.** **EULER'S CRITERION.** Let \( p \) be an odd prime and \( (a,p) = 1 \). Then \( a \) is a quadratic residue of \( p \) if and only if \( a^{(p-1)/2} \equiv 1 \pmod{p} \).

**PROOF:** Suppose that \( a \) is a quadratic residue of \( p \), i.e. \( x^2 \equiv a \pmod{p} \) admits a solution, call it \( x \). Since \( (a,p) = 1 \), evidently \( (x,p) = 1 \). We may therefore appeal to Fermat's Little Theorem (Lemma 6) to obtain
\[
a^{(p-1)/2} \equiv (x_1^2)^{(p-1)/2} \equiv x_1^{p-1} \equiv 1 \pmod{p}.
\]

For the opposite direction, assume that \( a^{(p-1)/2} \equiv 1 \pmod{p} \) holds and let \( r \) be a primitive root of \( p \). (Here, due to its place in history, we can accept the use of Euler's \( \phi \)-function, which we will accept without further proof or discussion. If \( r \phi(p) \equiv 1 \pmod{p} \), and \( \phi(p) \) is the smallest such \( k \) such that \( r^k \equiv 1 \pmod{p} \), then \( r \) is deemed a primitive root of \( p \). In our application, since \( p \) is a prime, we know that \( \phi(p) = p-1 \).) Then \( a \equiv r^k \pmod{p} \) for some integer \( k \), with \( 1 \leq k \leq p-1 \). It follows that

\[
r^{k(p-1)/2} \equiv a^{(p-1)/2} \equiv 1 \pmod{p}.
\]

By Lemma 5, the order of \( r \) (namely \( p-1 \)) must divide the exponent \( k(p-1)/2 \). (Note: The order of \( a \) modulo \( n \) is the smallest positive integer \( k \) such that \( a^k \equiv 1 \pmod{n} \).) The implication is that \( k \) is an even integer, say \( k = 2j \). Hence,

\[
(r^j)^2 = r^{2j} = r^k \equiv a \pmod{p},
\]

making the integer \( r^j \) a solution of the congruence \( x^2 \equiv a \pmod{p} \). This proves that \( a \) is a quadratic residue of the prime \( p \).

**Lemma 8.** **Gauss's Lemma.** Let \( p \) be an odd prime and let \( (a,p) = 1 \). If \( n \) denotes the number of integers in the set

\[ S = \{ a, 2a, 3a, \ldots, ((p-1)/2)a \} \]

whose remainders upon division by \( p \) exceed \( p/2 \), then
\[
\left(\frac{a}{p}\right) = (-1)^n.
\]

PROOF (Burton 1976): Since \((a,p) = 1\), none of the \((p-1)/2\) integers in \(S\) is congruent to zero and no two are congruent to each other \( \mod p \). Let \(r_1, r_2, \ldots, r_m\) be those remainders upon division by \(p\) such that \(0 < r_i < p/2\) and \(s_1, \ldots, s_n\) be those remainders such that \(p > s_i > p/2\). Then \(m + n = (p-1)/2\), and the integers
\[
r_1, \ldots, r_m, p - s_1, \ldots, p - s_n
\]
are all positive and less than \(p/2\).

In order to show that these integers are all distinct, it suffices to show that no \(p - s_i\) is equal to any \(r_j\). Assume to the contrary that
\[
p - s_i = r_j
\]
for some choice of \(i\) and \(j\). Then there exists integers \(u\) and \(v\), with \(1 \leq u, v \leq (p-1)/2\), satisfying \(s_i = ua \mod p\) and \(r_j = va \mod p\). Hence,
\[
(u + v)a = s_i + r_j \equiv p \equiv 0 \mod p
\]
which says that \(u + v \equiv 0 \mod p\). But the latter congruence cannot take place, since \(1 < u + v < p - 1\).

The point which we wish to bring out is that the \((p - 1)/2\) integers
\[
r_1, \ldots, r_m, p - s_1, \ldots, p - s_n
\]
are simply the integers \(1, 2, \ldots, (p - 1)/2\), not necessarily
in order of appearance. Thus their product is \( ((p - 1)/2)! \):

\[
((p - 1)/2)! = r_1 \ldots r_m(p - s_1) \ldots (p - s_n) \\
= r_1 \ldots r_m(-s_1) \ldots (-s_n) \pmod{p} \\
= (-1)^n r_1 \ldots r_m s_1 \ldots s_n \pmod{p}.
\]

But we know that \( r_1, \ldots, r_m, s_1, \ldots, s_n \) are congruent modulo \( p \) to \( a, 2a, \ldots, ((p - 1)/2)a \), in some order, so that

\[
((p - 1)/2)! = (-1)^n a \cdot 2a \cdot \ldots \cdot ((p - 1)/2)a \pmod{p} \\
= (-1)^n a^{(p-1)/2} ((p - 1)/2)! \pmod{p}.
\]

Since \( ((p - 1)/2)! \) is relatively prime to \( p \), it may be cancelled from both sides of this congruence to give

\[
1 = (-1)^n a^{(p-1)/2} \pmod{p}
\]
or, upon multiplying by \( (-1)^n \),

\[
a^{(p-1)/2} \equiv (-1)^n \pmod{p}.
\]

Use of Euler's Criterion (Lemma 7) now completes the argument:

\[
\left( \frac{a}{p} \right) = a^{(p-1)/2} = (-1)^n \pmod{p},
\]

which implies that

\[
\left( \frac{a}{p} \right) = (-1)^n.
\]

**EXAMPLE:** Let \( p = 19 \) and \( a = 7 \). Then \( (p - 1)/2 = 9 \), and

\[
S = \{ 7, 14, 21, 28, 35, 42, 49, 56, 63 \}
\]

Divide each of the above elements by 19. This would give us the remainders
7, 14, 2, 9, 16, 4, 11, 18, 6
of which 14, 16, 11, and 18 are greater than \( p/2 = 9.5 \).

Gauss's Lemma states then that
\[
\left( \frac{7}{13} \right) = (-1)^4 = 1.
\]

**Lemma 2** (Lagrange, 1775). If \( p \) is an odd prime, then:
\[
\left( \frac{2}{p} \right) = \begin{cases} 
1 & \text{if } p \equiv 1 \pmod{8} \text{ or } p \equiv 7 \pmod{8}; \\
-1 & \text{if } p \equiv 3 \pmod{8} \text{ or } p \equiv 5 \pmod{8}.
\end{cases}
\]

**Proof** (Burton 1976): According to Gauss's Lemma (Lemma 8),
\[
\left( \frac{2}{p} \right) = (-1)^n,
\]
where \( n \) is the number of integers in the set
\[
S = \{2, 2 \cdot 2, 3 \cdot 2, \ldots, (p-1)/2 \cdot 2\}
\]
which, upon division by \( p \), have remainders greater than \( p/2 \).

The members of \( S \) are all less than \( p \), so it suffices to count the number that exceed \( p/2 \). For \( 1 \leq k \leq (p-1)/2, 2k \leq p/2 \)
if and only if \( k < p/4 \). Thus, there are \( [p/4] \) integers less than \( p/2 \) (where \( [ \ ] \) denotes the greatest integer function), hence
\[
n = \frac{p-1}{2} - [p/4]
\]
integers which are greater than \( p/2 \).

Now we have four possibilities; for, any odd prime has one of the forms \( 8k + 1, 8k + 3, 8k + 5, \) or \( 8k + 7 \). A simple calculation shows that
if \( p = 8k + 1 \), then \( n = 4k - [2k + \frac{1}{2}] = 4k - 2k = 2k \),
if \( p = 8k + 3 \), then \( n = 4k + 1 - \lfloor \frac{2k + 3}{4} \rfloor = 4k + 1 - 2k = 2k + 1 \),

if \( p = 8k + 5 \), then \( n = 4k + 2 - \lfloor \frac{2k + 1 + \frac{1}{4}}{2} \rfloor = 4k + 2 - (2k + 1) = 2k + 1 \),

if \( p = 8k + 7 \), then \( n = 4k + 3 - \lfloor \frac{2k + 1 + 3/4}{2} \rfloor = 4k + 3 - (2k + 1) = 2k + 2 \).

Thus, when \( p \) is of the form \( 8k + 1 \) or \( 8k + 7 \), \( n \) is even and \( \left( \frac{2}{p} \right) = 1 \). On the other hand, when \( p \) assumes the form \( 8k + 3 \) or \( 8k + 5 \), \( n \) is odd and \( \left( \frac{2}{p} \right) = -1 \).

**Lemma 10.** If \( q = 2p + 1 \) is a prime, then

- \( q | M_p \) provided that \( q = 8k + 1 \),
- \( q | M_p + 2 \) provided that \( q = 8k + 3 \).

**Proof:** \( q \) must divide \( M_p \) or \( M_p + 2 \). For, by Fermat's Little Theorem,

\[
2^{q-1} - 1 \equiv 0 \pmod{p},
\]

but \( 2^{q-1} - 1 = (2^{(q-1)/2} - 1)(2^{(q-1)/2} + 1) = (2^p - 1)(2^p + 1) = (2^p - 1)(2^p - 1 + 2) = M_p(M_p + 2) \).

Thus, \( M_p(M_p + 2) \equiv 0 \pmod{p} \).

Now, \( q | M_p \) and \( q | M_p + 2 \) would imply that \( q | 2 \), a contradiction. Thus, \( q | M_p \) or \( q | M_p + 2 \).

Now \( q | M_p \) implies \( q | 2^p - 1 \) which implies that \( 2^p \equiv 1 \pmod{q} \). Since \( (2, q) = 1 \), we have, by Euler's Criterion (Lemma 7) that \( 2 \) is a quadratic residue of \( q \), or in terms of the
Legendre symbol,
\[ \left( \frac{2}{q} \right) = 1. \]

By Lemma 9, this is equivalent to saying that \( q = 8k \pm 1 \).

In a similar fashion, we see that \( q \mid M_p + 2 \) implies that \( q \mid 2^p - 1 + 2 = 2^p + 1 \), which implies that \( 2^p \equiv -1 \pmod{q} \). Again, by Euler's Criterion and Lemma 9, we have \( q = 8k \pm 3 \).

**THEOREM 6 (EULER).** Every divisor of \( M_p \), for \( p > 2 \), is of the form \( 8k \pm 1 \).

**PROOF (Shanks 1978):** Let \( q = 2Q + 1 \) be a prime divisor of \( M_p \).

Then,
\[ q \mid 2M_p = 2^{p+1} - 2 = n^2 - 2, \text{ where } N = 2^{(p+1)/2}. \]

Thus, \( q \mid N^2 - 2 \) implies \( qk = N^2 - 2 \) implies \( 2 = N^2 - qk \) for some integer \( k \).

Then, \( 2^2 = N^4 - k_2q \) for some integer \( k_2 \). \( (N^2 = 2 \pmod{q}) \) implies \( N^4 \equiv 4 \pmod{q} \).

By induction,
\[ 2^Q = N^{2Q} - Lq \text{ for some integer } L. \]

Now, \( q \nmid N \), since \( q \nmid 2 \), and thus, by Fermat's Little Theorem, \( q \mid N^{2Q} - 1 \), and, by Lemma 10, \( q \) must be of the form \( 8k \pm 1 \).

Finally, since a product of numbers of the form \( 8k \pm 1 \) is again of that form, all divisors of \( M_p \) are of that form.
Theorems 5 and 6 greatly reduce the number of qualifying prime divisors of $M_p$. Consider the two together:

Any prime which divides $M_p$ must be of the form $2kp + 1$

AND $8j + 1$.

Thus, reconsider Cataldi's 128 divisions necessary to determine the primality of $M_{19} = 524,287$:

1) He need consider only primes $< 524,287$ or $< 724,07665$ (of which there are 128). It can easily be shown that no perfect number is a perfect square, hence '<' is used instead of '<'.

2) Eliminate those not of the form $2kp + 1 = 38k + 1$.

That leaves just six: 191, 229, 419, 457, 571 and 647.

3) Of those six, only 191, 647 and 457 are of the form $8j + 1$.

While this looks extremely promising, its application is extremely limited, as we shall now see.

Shanks (1978) offers an excellent comparison of the number of divisions necessary by the various methods so far discussed (see Table 1). With his new theorem, Euler was able to determine the primality of $M_{31} = 2,147,483,647$. Even with this seemingly powerful tool, a glance at the bottom line of the table below shows the uselessness of Euler's method for any further discoveries of Mersenne primes, for the next one would take approximately 620,000 computations, after one determined what those 620,000 numbers were.

This brings us to the close of the "old age" of perfect number research. Euler's number wasn't surpassed for 104 years, when a French
mathematician, Francois Edouard Anatole Lucas, devised an ingenious method for testing the primality of Mersenne numbers which required no division at all.

**TABLE 1. THE FIRST NINE MERSENNE PRIMES**

<table>
<thead>
<tr>
<th>p</th>
<th>M_p</th>
<th>s_p</th>
<th>c_p</th>
<th>f_p</th>
<th>e_p</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>7</td>
<td>2</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>5</td>
<td>31</td>
<td>5</td>
<td>3</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>7</td>
<td>127</td>
<td>11</td>
<td>5</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>13</td>
<td>8,191</td>
<td>90</td>
<td>24</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>17</td>
<td>131,071</td>
<td>362</td>
<td>72</td>
<td>4</td>
<td>3</td>
</tr>
<tr>
<td>19</td>
<td>524,287</td>
<td>724</td>
<td>128</td>
<td>6</td>
<td>3</td>
</tr>
<tr>
<td>31</td>
<td>2,147,483,647</td>
<td>46,340</td>
<td>4,792</td>
<td>157</td>
<td>84</td>
</tr>
<tr>
<td>61</td>
<td>2,305,843,009,213,693,951</td>
<td>1.5 e9</td>
<td>76 e6</td>
<td>1.25 e6</td>
<td>.62 e6</td>
</tr>
</tbody>
</table>

- \( s_p = \lceil \sqrt{M_p} \rceil \)
- \( c_p = \pi[s_p] \) = the number of primes less than or equal to \( s_p \)
- \( f_p \) = number of primes of the form \( 2kp + 1 \) which are \( \leq s_p \)
- \( e_p \) = number of primes of the form \( 2kp + 1 \) and \( 8k + 1 \) which are \( \leq s_p \)

Note: the exponential numbers of the last row are estimates. (Shanks 1978)
Leonardo Pisano (or de Pisa), also known as Fibonacci (1180-1250?) was perhaps the best known of the Medieval mathematicians. Besides being credited with introducing Western Europe to the Hindu-Arabic method of numerical notation, he was also noted for the invention of continued fractions and for his famous problem on the offspring of rabbits:

How many pairs of rabbits will be produced in a year, beginning with a single pair, if in every month each pair bears a new pair which becomes productive from the second month on?

A substantial amount of study has been devoted over the centuries to Fibonacci's sequence generated by this problem, i.e.,

1, 1, 2, 3, 5, 8, 13, 21, ...

and related topics, even to the point of generating its own journal, The Fibonacci Quarterly.

Well over a century before Lucas' time it had been established that the numbers of Fibonacci's sequence were the denominators of the simple continued fraction convergents of the positive root of $x^2 = x + 1$.

To see this, consider a continued fraction representation of $x^2 = x + 1$, or $x = 1 + 1/x$. Substitution of the right-hand side into
the $x$ of the right-hand side gives us

$$x = 1 + \frac{1}{1 + \frac{1}{x}}.$$  

Repeated substitution of $1 + \frac{1}{x}$ gives us

$$x = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \ldots}}}.$$  

Since it can easily be shown that the roots of $x^2 = x + 1$ are $x = \frac{1}{2}(1 \pm \sqrt{5})$, and that the above expression is obviously positive, we must have the expression for $x = \frac{1}{2}(1 + \sqrt{5})$.

Now, the corresponding convergents for $\frac{1}{2}(1 + \sqrt{5})$, that is, the value of the above expression chopped off and evaluated at each '+' sign, are

$$\frac{1}{1}, \frac{2}{1}, \frac{3}{2}, \frac{5}{3}, \frac{8}{5}, \frac{13}{8}, \frac{21}{13}, \frac{34}{21}, \frac{55}{34}, \ldots.$$  

It was shown by J. P. M. Binet (Dickson 1971) by 1843 that the $n$th term of the Fibonacci's sequence is

$$U_n = \frac{1}{\sqrt{5}} \left[ \left( \frac{1 + \sqrt{5}}{2} \right)^n - \left( \frac{1 - \sqrt{5}}{2} \right)^n \right]$$

easily proved by induction.

Most schoolchildren eventually see this series, in one way or another, and most will be informed, or discover for themselves, that each term, beginning with the third, is equal to the sum of the previous two, i.e., $U_n = U_{n-1} + U_{n-2}$. Numerous other properties were established in the following centuries, including several of note by Lucas (Lucas 1876).
Lucas was however, also noted for his own recurring series, derived from and very similar to Fibonacci's. In an article in *Nouv. Corresp. Math.* (1876), Lucas offered up a sample of his series:

$$u_n = \frac{a^n - b^n}{a - b} \quad \text{and} \quad v_n = a^n + b^n = u_{2n}/u_n = u_{n+1} + u_{n+1},$$

where and b are the roots, previously mentioned, of $x^2 = x + 1$.

Lucas' $u_n$ also generated Fibonacci's sequence.

Lucas' work with $u_n$ and $v_n$ led him to the discovery of new techniques for determining the primality of numbers of certain forms. Lucas noted (Dickson 1971),

If the term of rank $A+1$ in Pisano's series is divisible by the odd number $A$ of the form $10p + 3$ and if no term whose rank is a divisor of $A + 1$ is divisible by $A$, then $A$ is a prime. If the term of rank $A - 1$ is divisible by $A = 10p + 1$ and if no term of rank a divisor of $A - 1$ is divisible by $A$, then $A$ is a prime.

In other words, if $M$ is of the form $10p + 3$, and $M|u_{M+1}$ but $M \nmid u_d$ for any $d$ such that $d|M + 1$, then $M$ is a prime.

With this new "theorem" (Lucas was reluctant to explicitly state his theorems, but instead usually chose to demonstrate their application), Lucas was able to ascertain the primality of $M_{127}$. Due to the condition of the form of $A$, this might help to explain why he missed detecting the primality of $M_{61}$, $M_{89}$ and $M_{107}$.

In a subsequent article that same year, Lucas again gave his $u_n$ and $v_n$, but this time had them denote the roots of the more general $x^2 - Px + Q = 0$, where $P$ and $Q$ are relatively prime integers (Lucas 1876). Among the several other theorems generated by this article was
one noting that

If \( u_{p+1} \) is divisible by \( p \), but no term of rank a

divisor or \( p + 1 \) is divisible by \( p \), then \( p \) is a prime.

In the article it is shown that \( M_{31} \) is prime and that \( M_{67} \) is

composite, contrary to the writings of Mersenne and general opinion

of the time. It should be noted however, that although Lucas' method

is sufficient for determining the primality of some forms of Mersenne

numbers, it was not known at the time if any of Lucas' various methods

were necessary. Hence, failure of a Lucas test does not necessarily

imply that the number is composite.

Referring back to his original definition of \( v_n \), Lucas defined

\[ r_n = v_{2^n} \]

and stated that if a number, \( M_p \), is of the form \( 4m + 3 \), then

\( M_p \) is prime if and only if \( M_p \mid r_{p-1} \) (Lucas 1876). It is not hard

to show that \( r_1 = 3 \), and \( r_n = r_{n-1}^2 \) for \( n > 1 \). This is commonly re-

ferred to as Lucas' Second Theorem. It appears in several articles,

both contemporously and subsequently, in many forms. It is however,

the foundation upon which D. H. Lehmer later built his unification of

Lucas' work.

Lucas published several more articles on his recurring series

and gave several more variations on his primality testing schemes.

The reader is referred to Dickson's book for a brief summary of these

ventures. Most of the original sources can still be found in the

archives of major universities with notable math research libraries.

Lucas' original articles were found by this author at Syracuse Uni-

versity, where much lament was given over my never haven taken my

French training seriously.
Lucas' various theorems were tried and tested over the ensuing years by a number of researchers. The primality of $M_{61}$ was established by J. Pervusin in 1883 and independently confirmed by P. Seelhoff in 1886. Ralph E. Powers (1875-1952) determined, using Lucas's Second Theorem, that $M_{89}$ was prime, in 1912. E. Fauquembergue gave a contemporaneous verification by writing out the mod 89 residues of that series to the base 2.

Fauquembergue's method brings to mind the necessity of working with modular arithmetic while computing the terms of Lucas' sequence. Noting that

\[
\begin{align*}
    u_1 &= 4 \\
    u_2 &= 14 \\
    u_3 &= 194 \\
    u_4 &= 37634 \\
    u_5 &= (\text{approximately}) 1.4163 \times 10^9 \\
    u_6 &= (\text{approximately}) 2.006 \times 10^{18} \\
\end{align*}
\]

and so on, ...

we would expect $u_{89}$ to be a totally unmanageable number, especially by hand methods or by using a primitive adding machine.

We must note however that we are not concerned primarily with the actual value, but whether or not that number is divisible by $M_p$; i.e., if $u_{p-1} \equiv 0 \pmod{M_p}$. Hence, by working with modular arithmetic we can reduce by mod $M_p$ at any step, primarily when the number exceeds $M_p$ (of course!). At first this does not seem like much of a trade-off, giving up multiplying numbers with hundreds of digits for division by an 87-digit number. Fortunately, we needn't determine the remainder
after each division by any act of division at all. There exists a simple application of modular arithmetic which makes this computation very simple, especially with today's high speed computers.

Consider the problem of squaring the number
\[ x = (a_n a_{n-1} \cdots a_0)_{\text{base } B} \]
subject to reduction modulo \( B^p - 1 \). The number of digits in \( x \) will be less than \( p \), else it would have already been reduced. By squaring \( x \) we would have a number of at most \( 2p \) digits. If this number is expressed in base \( B \), then we can consider reduction modulo \( B^p - 1 \) by considering \( x \) in two parts:
\[ x = (a_n a_{n-1} \cdots a_{p+1} a_p a_{p-1} \cdots a_2 a_1 a_0) \]
where \( p - 1 < n < 2p - 1 \).

If part 2 is less than \( B^p - 1 \), then the residue of part 2 modulo \( B^p - 1 \) is simply \((a_{p-1} \cdots a_2 a_1 a_0)\). If part 2 equals \( B^p - 1 \), then the residue modulo \( B^p - 1 \) is 0. By definition of part 2, it cannot exceed \( B^p - 1 \) in value.

It is not hard to show that for part 1, if we divide
\[ a_n B^n + a_{n-1} B^{n-1} + \cdots + a_{p+1} B^{p+1} + a_p B^p \]
by \( B^p - 1 \), we get
\[ a_n B^{n-p} + a_{n-1} B^{n-p-1} + \cdots + a_{p+1} B^1 + a_p \]
i.e., the same digits shifted \( B^p - 1 \) places to the right.

Therefore, the residue of \( x \) (mod \( B^p - 1 \)) is simply the sum of the first \( B^p - 1 \) digits (counting from the right) with the remaining \( B^p - 1 \) (at most) digits.
EXAMPLE:

\[(1010101)_{2} \pmod{2^4 - 1} \equiv (101)_{2} + (0101)_{2}
\]
\[\equiv (1010)_{2} \pmod{2^4 - 1}.
\]

EXAMPLE:

\[(12345678)_{10} \pmod{10^7 - 1} \equiv (1)_{10} + (2345678)_{10}
\]
\[\equiv (2345679)_{10} \pmod{10^7 - 1}.
\]

Note that by adding two p-digit numbers, we sometimes will get a p + 1 digit number, thus necessitating application of this idea again. It is easily shown that this can only happen once per reduction attempt.

EXAMPLE:

\[(11010101)_{2} \pmod{2^4 - 1} \equiv (1101)_{2} + (0101)_{2}
\]
\[\equiv (10010)_{2} \pmod{2^4 - 1}.
\]

Note that \((10010)_{2}\) is still greater than \(2^4 - 1\), so we still haven't achieved a proper residue. One more time,...

\[(10010)_{2} \pmod{2^4 - 1} \equiv (1)_{2} + (0010)_{2}
\]
\[\equiv (11)_{2} \pmod{2^4 - 1}.
\]
Most efforts in determining the primality of Mersenne numbers since 1930 have relied on the contributions of Derrick Henry Lehmer, a mathematics professor at the University of California at Berkeley. In an article entitled "An Extended Theory of Lucas' Functions" (Lehmer 1930), Lehmer consolidated the numerous disjunctive statements of Lucas into one **necessary and sufficient** statement. In a later article, Lehmer provided a rework of his proof in a simpler form, relying solely on elementary principals of number theory (Lehmer 1935). It is from this exposition that the following proof is derived, a couple of times removed.

Lucas demonstrated that the test described for the primality of numbers of the form $2^{4k+1} - 1$ (commonly referred to as Lucas' Second Test) was also valid for $2^{4k-1} - 1$, and that this was a necessary and sufficient condition. Numerous proofs have been offered, of which the following is taken from Roberts (1977). A. E. Western (1932) perhaps was the first to independently verify Lehmer's theorem, giving a proof by means of algebraic numbers. Irving Kaplansky (1945) gave a brief self-contained theorem in which he defines a function which admits Lucas' Second Test, and hence the Lucas-Lehmer Theorem, as a special case. Donald Knuth (1981) also offers a proof in his classic *The Art of Computer Programming* text.
THEOREM 7. THE LUCAS-LEHMER THEOREM. If \( p \) is an odd prime larger than 3, then \( M_p \) is prime if and only if \( M_p \mid S_{p-1} \), where \( S_1 = 4 \), \( S_{k+1} = S_k^2 - 2 \) for \( k \geq 1 \).

PROOF (Roberts 1977, with considerable detail added):

The proof will be delayed until after the presentation of much supporting work. The presentation is lengthy, though the mathematics involved is not difficult.

In the following discussion, we allow the expanded form of Lucas's \( u_n \) and \( v_n \) with the case \( a = 1 \) and \( b = \sqrt{3} \); i.e., for \( n = 1, 2, 3, 4, \ldots \), let

\[
\begin{align*}
  u_n &= \frac{1}{2 \sqrt{3}} [(1 + \sqrt{3})^n - (1 - \sqrt{3})^n] \\
  v_n &= (1 + \sqrt{3})^n + (1 - \sqrt{3})^n.
\end{align*}
\]

Thus, \( u_1 = 1 \) and \( v_1 = 2 \). It is easy to show that \( u_n \) and \( v_n \) are both integers and that \( v_n \) is always even. This is certainly the case for \( n = 1 \). For \( n > 1 \), we see that

\[
\begin{align*}
  u_{n+1} &= \frac{1}{2 \sqrt{3}} [(1 + \sqrt{3})^n(1 + \sqrt{3}) - (1 - \sqrt{3})^n(1 - \sqrt{3})] \\
  &= \frac{1}{2 \sqrt{3}} [(1 + \sqrt{3})^n + \sqrt{3}(1 + \sqrt{3})^n - (1 - \sqrt{3})^n + \\
  &\quad + \sqrt{3}(1 - \sqrt{3})^n] \\
  &= \frac{1}{2 \sqrt{3}} [(1 + \sqrt{3})^n - (1 - \sqrt{3})^n + \sqrt{3}(1 + \sqrt{3})^n - \\
  &\quad - (1 - \sqrt{3})^n] = \frac{1}{2 \sqrt{3}} [(1 + \sqrt{3})^n - (1 - \sqrt{3})^n + \sqrt{3} v_n] \\
  &= \frac{1}{2 \sqrt{3}} [(1 + \sqrt{3})^n - (1 - \sqrt{3})^n + \frac{1}{2} v_n] \\
  &= u_n + \frac{1}{2} v_n.
\end{align*}
\]

Therefore, if \( u_n \) and \( v_n \) are both integers, while \( v_n \) is even, then \( u_{n+1} \) is also an integer.

To support the "\( v_n \) is even" statement, we note that

\[
v_{n+1} = (1 + \sqrt{3})^n(1 + \sqrt{3}) + (1 - \sqrt{3})^n(1 - \sqrt{3})
\]

\[
= (1 + \sqrt{3})^n + \sqrt{3}(1 + \sqrt{3})^n - \sqrt{3}(1 - \sqrt{3})^n
\]

\[
= (1 + \sqrt{3})^n + (1 - \sqrt{3})^n + \sqrt{3}(1 + \sqrt{3})^n -
\]

\[
(1 - \sqrt{3})^n
\]

\[
= v_n + 6u_n.
\]

Therefore, if \( u_n \) and \( v_n \) are both integers, while \( v_n \) is even, then \( v_{n+1} \) is also even.

**LEMMA 11.** For all \( m \geq 1, n \geq 1 \)

\( a) \ 2u_{m+n} = u_m v_n + v_m u_n \)

\( b) \ (-2)^{m+1} = u_m v_{m+n} - v_m u_{m+n} \)

\( c) \ 2v_{m+n} = v_m v_n + 12u_m u_n \)

\( d) \ u_{2n} = u_n v_n \)

\( e) \ v_{2n} = v_n^2 + (-2)^{n+1} \)

\( f) \ v_n^2 - 12u_n^2 = (-2)^{n+2} \)

**PROOF OF PART A:**

\[
um v_n + v_m u_n = \frac{(a^m - b^m)(a^n + b^n)}{2\sqrt{3}}
\]

\[
+ \frac{(a^m + b^m)(a^n - b^n)}{2\sqrt{3}}
\]

where \( a = (1 + \sqrt{3}), \ b = (1 - \sqrt{3}) \), for brevity,

\[
= (a^{m+n} + a^m b^n - b^m a^n - b^{m+n} + a^m b^n + b^m a^n -
\]

\[
b^{m+n}) \frac{1}{2\sqrt{3}}
\]

\[
= 2(a^{m+n} - b^{m+n}) \frac{1}{2\sqrt{3}}
\]

\[
= 2u_{m+n}
\]
PROOF OF PART B: \[ u_n v_{m+n} = \frac{1}{2 \sqrt{3}} \left[ (1 + \sqrt{3})^m - (1 - \sqrt{3})^m \right](1 + \sqrt{3})^{m+n} + (1 - \sqrt{3})^{m+n} - \left[ (1 + \sqrt{3})^m + (1 - \sqrt{3})^m \right]. \]

\[ = \frac{1}{2 \sqrt{3}} \left[ (1 + \sqrt{3})^m \left( 1 + \sqrt{3} \right)^{m+n} - (1 - \sqrt{3})^m \left( 1 + \sqrt{3} \right)^{m+n} + (1 - \sqrt{3})^m \left( 1 - \sqrt{3} \right)^{m+n} - (1 + \sqrt{3})^m \left( 1 - \sqrt{3} \right)^{m+n} \right] \]

\[ = \frac{1}{2 \sqrt{3}} \left[ -2(1 - \sqrt{3})^m (1 + \sqrt{3})^{m+n} + 2(1 + \sqrt{3})^m \right]. \]

\[ = \frac{1}{2 \sqrt{3}} \left[ -2(1 - \sqrt{3})^m (1 + \sqrt{3})^{m+n} \right] \]

\[ = - \frac{1}{\sqrt{3}} (1 - \sqrt{3})(1 + \sqrt{3})^m \left[ (1 + \sqrt{3})^n - (1 - \sqrt{3})^n \right] \]

\[ = - \frac{(-2)^m}{\sqrt{3}} \left[ (1 + \sqrt{3})^n - (1 - \sqrt{3})^n \right] \]

\[ = (-2)^m (-2) \left[ (1 + \sqrt{3})^n - (1 - \sqrt{3})^n \right] \]

\[ = (-2)^{m+1} u_n. \]

PROOF OF PART C: \[ v_n v_n + 12 u_n u_n = \left[ (1 + \sqrt{3})^m + (1 - \sqrt{3})^m \right](1 + \sqrt{3})^n + \]

\[ + (1 - \sqrt{3})^n] + 12 \cdot \frac{1}{2 \sqrt{3}} \left[ (1 + \sqrt{3})^m - (1 - \sqrt{3})^m \right]. \]
\[
\frac{1}{2\sqrt{3}}\left[(1 + \sqrt{3})^n - (1 - \sqrt{3})^n\right]
\]
\[
= (1 + \sqrt{3})^{m+n} + (1 + \sqrt{3})^m(1 - \sqrt{3})^n + (1 - \sqrt{3})^m.
\]
\[
\cdot (1 + \sqrt{3})^n + (1 - \sqrt{3})^{m+n} + \frac{12}{2\cdot2\sqrt{3}\cdot\sqrt{3}}\left[(1 + \sqrt{3})^{m+n} - (1 - \sqrt{3})^n(1 + \sqrt{3})^m - (1 - \sqrt{3})^n\right].
\]
\[
\cdot (1 + \sqrt{3})^n + (1 - \sqrt{3})^{m+n}
\]
\[
= 2[(1 + \sqrt{3})^{m+n} + (1 - \sqrt{3})^{m+n}]
\]
\[
= 2v_{m+n}.
\]

**Proof of Part D:**
\[
u_n v_n = \frac{1}{2\sqrt{3}}\left[(1 + \sqrt{3})^n - (1 - \sqrt{3})^n\right]\left[(1 + \sqrt{3})^n + (1 - \sqrt{3})^n\right]
\]
\[
= \frac{1}{2\sqrt{3}}\left[(1 + \sqrt{3})^{2n} + (1 - \sqrt{3})^{2n}\right]
\]
\[
= u_{2n}.
\]

**Proof of Part E:**
\[
v_n^2 = \left[(1 + \sqrt{3})^n + (1 - \sqrt{3})^n\right]^2
\]
\[
= (1 + \sqrt{3})^{2n} + 2(1 + \sqrt{3})^n(1 - \sqrt{3})^n + (1 - \sqrt{3})^{2n}
\]
Thus,
\[
v_n^2 + (-2)^{n+1} = (1 + \sqrt{3})^{2n} + (1 - \sqrt{3})^{2n} + (-2)^{n+1} + 2(-2)^n
\]
\[
= (1 + \sqrt{3})^{2n} + (1 - \sqrt{3})^{2n} + (-2)(-2 + 2)
\]
\[
= (1 + \sqrt{3})^{2n} + (1 - \sqrt{3})^{2n}
\]
\[
= v_{2n}.
\]

**Proof of Part F:** By part (c), we know that
\[
2v_{m+n} = v_m v_n + 12u_m u_n
\]
for all positive integers $m$ and $n$. 
Let \( n = m \).

Then, \( 2v_{2n} = v_n^2 + 12u_n^2 \).

By part (e), we know that \( v_{2n} = 2v_n^2 + 2(-2)^{n+1} \).

Thus,

\[
2v_{2n} = 2v_n^2 + 2(-2)^{n+1}.
\]

Equating these last two results, we arrive at

\[
v_n^2 + 12u_n^2 = 2v_n^2 + 2(-2)^{n+1}
\]

or \( v_n^2 - 12u_n^2 = (-2)^{n+2} \).

**Lemma 12.** If \( p \) is a prime larger than 3, then

a) \( u_p \equiv \binom{3}{p} \pmod{p} \), (Lagrange symbol implied)

b) \( v_p \equiv 2 \pmod{p} \),

c) \( p | u_{p-1} u_{p+1} \).

**Proof of Part a:**

\[
 u_p = \frac{1}{2 \sqrt{3}} \left( \sum_{j=0}^{p} \binom{p}{j} \sqrt{3}^j - \sum_{j=0}^{p} \binom{p}{j} (-1)^j \sqrt{3}^j \right) \quad \text{(expansion of } (1 + \sqrt{3}) \text{ and } (1 - \sqrt{3}) \text{)}
\]

\[
= \sum_{j=0}^{D} \binom{p}{j} \sqrt{3}^{j-1} \equiv 3^{(p-1)/2} \equiv \binom{3}{p} \pmod{p}, \quad \text{by Euler's Criterion (Lemma 7).}
\]

In other words,

\[
 u_p = \frac{1}{2 \sqrt{3}} \sum_{j=0}^{p} (1 + \sqrt{3})^j - (1 - \sqrt{3})^j
\]

\[
= \frac{1}{2 \sqrt{3}} \sum_{j=0}^{p} \binom{p}{j} \sqrt{3}^j - \binom{p}{j} (-1)^j \sqrt{3}^j
\]

\[
= \frac{1}{2 \sqrt{3}} \left[ \sum_{j=0}^{p} \binom{p}{j} \sqrt{3}^j \right] - \frac{1}{2 \sqrt{3}} \left[ \sum_{j, \text{odd}} \binom{p}{j} \sqrt{3}^j \right] + \frac{1}{2 \sqrt{3}} \left[ \sum_{j, \text{odd}} \binom{p}{j} \sqrt{3}^j \right]
\]
Now, \( \binom{p}{k} \equiv 0 \pmod{p} \) for \( 1 \leq k \leq p-1 \), so we lose all but the last term. Don't believe that, huh? Note that

\[
k! \binom{p}{k} = k! \frac{p!}{k!(p-k)!} = p(p-1)(p-2) \ldots (p-k+1) \equiv 0 \pmod{p}.
\]

Thus \( p \mid k! \) or \( p \mid \binom{p}{k} \). But \( p \) cannot divide \( k! \). That would imply that \( p \mid j \) for some \( 1 \leq j \leq k \leq p-1 \). Can't have that. Therefore \( p \mid \binom{p}{k} \) or \( \binom{p}{k} = 0 \pmod{p} \).

Thus,

\[
\nu_p = 3^{(p-1)/2},
\]

and by Euler's Criterion (Lemma 7), we have

\[
3^{(p-1)/2} = \binom{3}{p} \pmod{p}.
\]

**PROOF OF PART B:** In a similar manner,

\[
\nu_p = \sum_{j=0}^{p} \binom{p}{j} \sqrt{3}^j + \sum_{j=0}^{p} \binom{p}{j} (-1)^j \sqrt{3}^j.
\]
\[
\sum_{j=0}^{p} \binom{p}{j} \sqrt[p]{3}^j - \left( \sum_{j=0}^{p} \binom{p}{j} \sqrt[p]{3}^j + \sum_{j=0}^{p} \binom{p}{j} \sqrt[p]{3}^j + \left( \sum_{j=0}^{p} \binom{p}{j} \sqrt[p]{3}^j \right) \right)
\]

= \sum_{j=0}^{p} \binom{p}{j} \sqrt[p]{3}^j

\]

= 2 \left( \binom{p}{0} \sqrt[p]{3}^0 + \binom{p}{2} \sqrt[p]{3}^2 + \binom{p}{4} \sqrt[p]{3}^4 + \ldots + \binom{p}{p-1} \sqrt[p]{3}^{p-1} \right).

Again, \( \binom{p}{k} = 0 \pmod{p} \) for \( 1 \leq k \leq p - 1 \).

Thus, \( \sqrt[p]{3} = 2 \left( \binom{p}{0} \sqrt[p]{3}^0 \pmod{p} = 2(1 \cdot 1) \pmod{p} = 2 \pmod{p} \right) \).

PROOF OF PART C: As previously noted, \( u_{n+1} = u_n + \frac{1}{2} v_n \).

Thus,

\[
\begin{align*}
\frac{1}{2} v_n = u_{n+1} - u_n, \\
2u_{n+1} = 2u_n + v_n.
\end{align*}
\]

By Lemma 11(b),

\[
(-2)^{m+1} u_m = u_m v_{m+n} - v_m u_{m+n}.
\]

Using \( m = 1 \) and \( n = p - 1 \), this becomes

\[
(-2)^2 u_{p-1} = u_1 v_{1+p-1} - v_1 u_{1+p-1}, \quad \text{or}
\]

\[
4u_{p-1} = u_1 v_1 - v_1 u_p.
\]

Noting that \( u_1 = 1 \) and \( v_1 = 2 \), we thus arrive at

\[
4u_{p-1} = v_1 - 2u_p.
\]

Multiplying equation (8) by equation (9), we get

\[
8u_{p+1}u_{p-1} = -4u_p^2 + v_p^2.
\]
Now, by part (a), we see that
\[ u_p = \left( \frac{3}{p} \right) \equiv -1 \pmod{p} \text{ or } +1 \pmod{p} \]
(depending on whether 3 is a quadratic residue of p or not.)
In either case,
\[ u_p^2 = (\pm 1)^2 \equiv 1 \pmod{p}. \]

Now, by part (b), we see that \( v_p^2 \equiv 4 \pmod{p} \). Thus,
\[ 8u_p u_{p-1} \equiv -4 \cdot 1 + 4 \pmod{p} \equiv 0 \pmod{p}. \]
Therefore, since p cannot divide 8, we must have
\[ p | u_{p+1} u_{p-1}, \] by the Corollary to Lemma 3.

**Lemma 13.** If p is a prime larger than 3 and \( S_p \) is the set of integers n for which \( p | u_n \), then:

a) m, n in \( S_p \) imply m + n is in \( S_p \),
b) m, n in \( S_p \) and n < m imply m - n is in \( S_p \),
c) if \( w_p \) is the smallest element of \( S_p \), then
   1) \( w_p \leq p + 1 \),
   2) n is in \( S_p \) if and only if \( w_p | n \).

**Proof of Part A:** By Lemma 11 (a), we know that \( 2u_{m+n} = u_m v_n + v_m u_n \).

Now, \( p | u_m \) implies \( p | u_m v_n \), and \( p | u_n \) implies \( p | v_m u_n \); therefore
\[ p | u_m v_n + v_m u_n = 2u_{m+n}. \]

Since p, a prime greater than 3, cannot divide 2, we must have
\[ p | u_{m+n}, \text{ i.e., } m + n \text{ is in } S_p. \]
PROOF OF PART B: By Lemma 11 (b), we know that \((-2)^{m+n}u_n = u_m \cdot v_{m+n} - v_m u_{m+n}\) for all positive integers, \(m\) and \(n\). Certainly this holds for the substitution of the integer \(m - n\) for \(n\), provided that \(m - n > 0\).

Thus,
\[\ (-2)^{m+n}u_{m+n} = u_m \cdot v_{2m} - v_m u_{2m}\]

By Lemma 11 (d), \(u_{2m} = u_m \cdot v_m\). Since \(p \mid u_m\), then \(p \mid u_{2m}\).

Thus, \(p \mid (-2)^{m+n}u_{m+n}\).

Since \(p\) is a prime \(> 3\) and thus cannot divide \((-2)^{m+n}\), we must have \(p \mid u_{m+n}\), i.e., \(m - n\) is in \(S_p\), again by the Corollary to Lemma 3.

PROOF OF PART C (1): By Lemma 12 (c), \(p \mid u_{p-1}u_{p+1}\).

Since \(p\) is a prime, then by the Corollary to Lemma 3, \(p \mid u_{p-1}\) or \(p \mid u_{p+1}\). In the first case, \(p - 1\) must be an element of \(S_p\), thus \(w_p \leq p - 1 \leq p + 1\).

The latter case is trivial.

PROOF OF PART C (2): Let \(w_p \mid n\).

Then, \(qw_p = n\) for some positive integer \(q\).

By part (a) and by induction on \(i\), we have \(iw_p\) is in \(S_p\) for all positive integers \(i\). Thus \(qw_p\) is in \(S_p\), i.e., \(p \mid u_n\).

Going the other way, we let \(n\) be in \(S_p\) while \(w_p \nmid n\). Then \(m = qw_p + r\) for some \(0 < r < w_p\).

By the previous argument, \(qw_p\) is in \(S_p\). By part (b), \(n > qw_p; n, qw_p\) both in \(S_p\) imply that \(n - qw_p = r\) is also in \(S_p\).
But since \( r < w_p \), we have a contradiction to the fact that \( w_p \) is the smallest such element. Hence, \( w_p \) must divide \( n \) after all.

**Lemma 14.** There are integers \( S_1, S_2, \ldots \) such that
\[
S_1 = 4, \ S_{k+1} = S_k^2 - 2 \ \text{for} \ k \geq 1, \ \text{and}
\]
\[
v_k = 2^{\frac{2^k-1}{2}} \cdot S_k \ \text{for} \ k \geq 1.
\]

**Proof:** By definition, \( v_2 = 8 \). Now, \( 8 = 2^{2^1-1} \cdot 4 \), so put \( S_1 = 4 \).

By Lemma 11 (e), \( v_{2n} = v_n^2 + (-2)^{n+1} \). Let \( n = 2^k \). Then,
\[
v_{2^k} = v_2^2 + (-2)2^k \]
\[
v_{2^{k+1}} = v_{2^k}^2 + (-2)2^{k+1} = 2^{k}S_k^2 + (-2)2^{k+1}
\]
\[= 2^k(S_k^2 - 2).\]
So we put \( S_{k+1} = S_k^2 - 2 \).

**Lemma 15.** If \( q \) is an odd prime and \( p \) is a prime divisor of \( M_q \), which in turn, divides \( v_{2^{q-1}} \), then
\[
a) \ p > 3, \ \ \ \ \ \ \ \ d) \ w_p \nmid w_{q-1} \]
\[
b) \ p \mid u_{2^q} \quad \quad \quad \ \ d) \ w_p = 2^q \]
\[
c) \ w_p \mid 2^q \ \ \ \ \ \ \ \ \ \ f) \ p = M_q \]

**Proof of Part A:** Since \( M_q = 2^q - 1 = (-1)^q - 1 \equiv -2 \pmod{3} \), we see that \( p \neq 3 \), otherwise \( M_q \equiv 0 \pmod{3} \).
PROOF OF PART B: From Lemma 11 (d), we know that \( u_{2n} = u_n v_n \). Substituting \( 2^{q-1} \) for \( n \) we get
\[
\frac{u}{2^q} = \left( \frac{u}{2^{q-1}} \right) \left( \frac{v}{2^{q-1}} \right).
\]

Since \( p \mid \frac{v}{2^{q-1}} \), we can conclude that \( p \mid \frac{u}{2^q} \).

PROOF OF PART C: From part (b), \( 2^q \) is in \( S_0 \). So, by Lemma 13 (c) (2), \( w_p \mid 2^q \).

PROOF OF PART D: If \( w_p \mid 2^{q-1} \), then by Lemma 13 (c) (2), \( 2^{q-1} \) is in \( S_p \).

Thus \( p \mid \frac{u}{2^{q-1}} \) and by Lemma 11 (f) we conclude \( p \mid (2)^{2^{q-1} + 2} \), a contradiction. \( 2^{q-1} + 2 \) (with \( q \), an odd prime) is always even.

Thus, \((-2)^{2^{q-1} + 2}\) is always a positive power of 2. \( p \) can divide a power of 2 if and only if \( p \) is itself a power of 2 to some degree. But, by part (a), \( p \) is a prime > 3, wherein the contradiction arises.

PROOF OF PART E: This follows immediately from parts (c) and (d), for if \( w_p \mid 2^q \) while \( w_p \mid 2^{q-1} \), we must have \( w_p = 2^q \).

PROOF OF PART F: By Lemma 13 (c) (1) and part (e), we know that \( w_p = 2^q \leq p + 1 \); thus \( M_q = 2^q - 1 \leq p \); but \( p \leq M_q \) (since \( p \) is a prime divisor of \( M_q \)). Therefore, \( M_q \) must equal \( p \).

**Lemma 16.** Let \( p \) be an odd prime other than 3 and suppose \( a = 3 \). Then,

a) \( V \) is the number of \( j \), \( 1 \leq j \leq \frac{p-1}{2} \), for which
\[
\frac{p}{2} < 3j < p,
\]
b) $V = \left[ \frac{p}{3} \right] - \left[ \frac{p}{6} \right] = \begin{cases} 0 \pmod{2} & \text{if } p \equiv \pm 1 \pmod{12} \\ 1 \pmod{2} & \text{if } p \equiv \pm 5 \pmod{12} \end{cases}$

where the brackets represent the greatest integer function,

where the brackets represent the greatest integer function,

c) $3$ is a quadratic residue of all $12k + 1$ primes and a quadratic non-residue of all $12k + 5$ primes.

**PROOF OF PART A:** The least absolute mod $p$ residues of $a, 2a, \ldots, ((p - 1)/2)a$ which lie between $-(p/2)$ and $p/2$ will be denoted by $a_1, a_2, \ldots, a_{(p-1)/2}$. Let $V$ be the number of $a_1, \ldots, a_{(p-1)/2}$ which are negative. (Thus, the variable 'V' in this Lemma is identical with the variable 'n' of Gauss's Lemma (Lemma 8).)

**EXAMPLE:** If $a = 3$ and $p = 37$, then the least absolute mod $p$ residues of $3, 6, 9, \ldots, (3/2)(37 - 1) = 54$ which lie between $-37/2$ and $37/2$ can be determined by inspection:

<table>
<thead>
<tr>
<th>least positive residue (mod 37)</th>
<th>least negative residue (mod 37)</th>
<th>least absolute residue (mod 37)</th>
</tr>
</thead>
<tbody>
<tr>
<td>3</td>
<td>40</td>
<td>-34</td>
</tr>
<tr>
<td>6</td>
<td>43</td>
<td>-31</td>
</tr>
<tr>
<td>9</td>
<td>46</td>
<td>-28</td>
</tr>
<tr>
<td>12</td>
<td>49</td>
<td>-25</td>
</tr>
<tr>
<td>15</td>
<td>52</td>
<td>-22</td>
</tr>
<tr>
<td>18</td>
<td>55</td>
<td>-19</td>
</tr>
<tr>
<td>21</td>
<td>58</td>
<td>-16</td>
</tr>
<tr>
<td>24</td>
<td>61</td>
<td>-13</td>
</tr>
<tr>
<td>27</td>
<td>64</td>
<td>-10</td>
</tr>
<tr>
<td>30</td>
<td>67</td>
<td>-7</td>
</tr>
<tr>
<td>33</td>
<td>70</td>
<td>-4</td>
</tr>
<tr>
<td>36</td>
<td>73</td>
<td>-1</td>
</tr>
<tr>
<td>39</td>
<td>2</td>
<td>-35</td>
</tr>
<tr>
<td>42</td>
<td>5</td>
<td>-32</td>
</tr>
<tr>
<td>45</td>
<td>8</td>
<td>-29</td>
</tr>
<tr>
<td>48</td>
<td>11</td>
<td>-26</td>
</tr>
<tr>
<td>51</td>
<td>14</td>
<td>-23</td>
</tr>
<tr>
<td>54</td>
<td>17</td>
<td>-20</td>
</tr>
</tbody>
</table>
Looking at the last column, we see six numbers that lie between \(-37/2\) and \(37/2\), i.e., -16, -13, -10, -7, -4, and -1. Thus \(V = 6\).

It is clear in our application that \(p < 3a < (3/2)(p - 1)\) must have positive residues in the interval \((0, p/2)\), which, thus, are the least absolute residues. Similarly, for \(p/2 < 3a < p\), we have negative residues in the interval \((-p/2, 0)\). Our conclusion is immediate, save for notation, using a 'j' as the index instead of an 'a'.

**PROOF OF PART B:** When \(a > b\), \([a] - [b]\) is the number of integers, \(m\), satisfying \(b < m \leq a\), i.e., in this case, \(p/6 < m \leq p/3\).

By part (a), \(V\) is the number of \(j\), \(1 \leq j \leq (p - 1)/2\) for which \(p/2 < 3j < p\); thus \(V = \lfloor p/3 \rfloor - \lfloor p/6 \rfloor\).

Considering \(p\) to be of the form \(12k + i\), we have

\[
V = \lfloor p/3 \rfloor - \lfloor p/6 \rfloor \quad \begin{cases} 
0 \pmod{2} & \text{if } i = 1 \text{ or } 11, \\
i.e., i + 1 \pmod{12}, & \\
1 \pmod{2} & \text{if } i = 5 \text{ or } 7, \\
i.e., i + 5 \pmod{12}.
\end{cases}
\]

**PROOF OF PART C:** By the Lemma of Gauss (Lemma 8):

\[
\left( \frac{a}{p} \right) = (-1)^V \text{ where } V \text{ is the number of } a_1, \ldots, a_{(p-1)/2} \text{ which are negative.}
\]

Recall:

\[
\left( \frac{a}{p} \right) = \begin{cases} 
1 & \text{if } a \text{ is a quadratic residue of } p, \\
-1 & \text{if } a \text{ is a quadratic non-residue of } p.
\end{cases}
\]
Thus,

$$\left( \frac{3}{p} \right) = \begin{cases} 1 & \text{if } 3 \text{ is a quadratic residue of } p, \\ -1 & \text{if } 3 \text{ is a quadratic non-residue of } p. \end{cases}$$

However, $$\left( \frac{3}{p} \right) = (-1)^V$$, by the Lemma of Gauss ($p$ is an odd prime and we assume that $3$ does not divide $p$).

Thus, since

$$V = \begin{cases} 0 \pmod{2} & \text{if } p \equiv \pm 1 \pmod{12} \\ 1 \pmod{2} & \text{if } p \equiv \pm 5 \pmod{12} \end{cases},$$

by part (b), then

$$\left( \frac{3}{p} \right) = -1^0 = 1 \quad \text{if } V \equiv 0, \text{ i.e., if } p \equiv \pm 1 \pmod{12},$$

implying that $3$ is a quadratic residue of $12k + 1$ primes,

$$\left( \frac{3}{p} \right) = -1^1 = -1 \quad \text{if } V \equiv 1, \text{ i.e., if } p \equiv \pm 5 \pmod{12},$$

implying that $3$ is a quadratic non-residue of $12k + 5$ primes.

**Lemma 17.** If $M_p = 2^p - 1$ is prime, then

a) $$2^p v = 2^p v_{2^p-1} + 12u^{2^p-1} \equiv -8 \pmod{M_p}$$

b) $$v_{2^p} = v_{2^p-1}^2 - 4 \cdot 2^{2^p-1} - 1,$$

c) $$v_{2^p-1}^2 = 4 (2^{(M_p-1)/2} - 1) \pmod{M_p},$$

d) $$M_p \mid v_{2^p-1}.$$

**Proof of Part A:** From Lemma 11 (c), $$2^v_{m+n} = v_m v_n + 12u_m u_n.$$ Let $m = 2^p - 1$, $n = 1$. Then, $$2^v_{m+n}$$ becomes $$2^v_{2^p-1} v_1 + 12u_{2^p-1} u_1.$$
Now, by definition, \( v_1 = 2, u_1 = 1 \), which implies that

\[
2v = 2v \cdot 2^{p-1} + 12u \cdot 2^{p-1}
\]

\[
\left[ 4 + 12 \left( \frac{3}{2^{p-1}} \right) \right] \pmod{2^p - 1}
\]

by Lemma 12 (a) and 12 (b), respectively.

Now, \( 2^5 \equiv 8 \pmod{12} \). Assume \( 2^s \equiv 8 \pmod{12} \) for some \( s \), i.e., \( 12x = 2^s - 8 \) for some \( x \). Then

\[
12 \cdot 4x = 4(2^s - 8) = (2^{s+2} - 8) - 24
\]

\[
12 \cdot 4x + 24 = 2^{s+2} - 8
\]

\[
12(4x + 2) = 2^{s+2} - 8.
\]

Therefore, \( 12 | 2^{s+2} - 8 \), or \( 2^{s+2} \equiv 8 \pmod{12} \).

Thus, by induction, all odd integers larger than 3 satisfy \( 2^s \equiv 8 \pmod{12} \).

Hence, \( 2^s - 1 \equiv 7 \pmod{12} \) \( \equiv -5 \pmod{12} \).

So, ... if \( 2^s - 1 \) is a prime, then by Lemma 16 (c), 3 is a quadratic non-residue of \( 2^s - 1 \), or in terms of the Legendre symbol,

\[
\left( \frac{3}{2^s-1} \right) = -1;
\]

consequently, \( \left( \frac{3}{2^p-1} \right) = -1 \) and for all \( s \), odd \( > 3 \),

\[
2v \cdot 2^p \equiv \left[ 4 + 12 \left( \frac{3}{2^{p-1}} \right) \right] \pmod{2^p - 1}, \text{ or}
\]

\[
2v \cdot 2^p \equiv (4 - 12) \pmod{2^p - 1} \equiv -8 \pmod{M_p}.
\]

**PROOF OF PART B:** By Lemma 11 (e), for \( m \geq 1, n \geq 1 \), \( v_{2n} = v_n^2 + (-2)^{n+1} \).

Let \( n = 2^{p-1} \). Then
\[ v_{2(2^p-1)} = v_{2^p-1}^2 + (-2)^{2^p-1} + 1 = v_{2^p-1}^2 + \]
\[ + (-2)^{2^p-1-1} + 2 \]
\[ = v_{2^p-1}^2 - 4 \cdot 2^{2^p-1-1}. \]

Thus,
\[ v_{2^p} = v_{2^p-1}^2 - 4 \cdot 2^{2^p-1-1}. \]

PROOF OF PART C: By part (a) we know that if \( M_p = 2^p - 1 \) is prime, then \( 2v_{2^p} \equiv -8 \pmod{M_p} \). Thus, \( M_p \mid 2v_{2^p} + 8 \), or \( xM_p = 2v_{2^p} + 8 \) for some integer \( x \). \( (M_p, \) an odd prime in our application, \( p > 3 \) imply that \( x \) is even, since the right hand side is even).

Thus, \( 2yM_p = 2v_{2^p} + 8 \) for some integer \( y \), not necessarily even. So, we have
\[ yM_p = v_{2^p}^2 + 4 = v_{2^p-1}^2 - 4 \cdot 2^{2^p-1-1} + 4 \pmod{M_p} \]
(by part (b))
\[ = v_{2^p-1}^2 - 4(2^{2^p-1-1-1}). \]

Therefore,
\[ v_{2^p-1}^2 = 4\left(\frac{2^{2^p-1-1}}{2} - 1\right) \pmod{M_p} \]
\[ = 4\left(\frac{M_p - 1}{2} - 1\right) \pmod{M_p}. \]

PROOF OF PART D: To show that \( M_p \mid v_{2^p-1}^2 \), it would be handy to use part (c) with the condition that \( 2^{p-1} \equiv 1 \pmod{M_p} \).
Thus, $v^2_{2^{p-1}}$ would be congruent to $4(1 - 1)$ (mod $M_p$) which is congruent to 0 (mod $M_p$). This implies that $M_p | v^2_{2^{p-1}}$ and $M_p | v_{2^{p-1}}$, for, by Euler's Criterion (Lemma 7),

$$\left(\frac{2}{M_p}\right) = 2^{(M_p-1)/2} \pmod{M_p}.$$ 

Lemma 9 tells us that $\left(\frac{2}{M_p}\right) = 1$ if and only if $p \equiv \pm 1 \pmod{8}$, and Theorem 6 demonstrates that all divisors of $M_p$ are of that form.

Thus,

$$v^2_{2^{p-1}} = 0 \pmod{M_p} \text{ and } M_p | v_{2^{p-1}}.$$ 

We are now in a position to establish the Lucas-Lehmer Theorem:

PROOF OF THEOREM 7: If $M_p$ is prime then, by Lemma 17 (d), $M_p | v_{2^{p-1}}$ and therefore, by Lemma 14, $M_p | S_{p-1}$, i.e.,

$$M_p | v_{2^{p-1}} \implies M_p | 2^{2^{p-1}-1}.$$ 

Since $M_p \not| 2^{2^{p-1}-1}$ ($M_p$ is prime; $2^{2^{p-1}-1}$ is a power of 2 $\geq 256$; $p > 3$ all imply that $M_p \neq 2$), we must have $M_p | S_{p-1}$ by the Corollary to Lemma 3.

On the other hand, any prime divisor of $M_p$ must, when $M_p$ divides $v_{2^{p-1}}$ (which is true when $M_p | S_{p-1}$ (i.e., $M_p | S_{p-1}$, $S_{p-1} | v_{2^{p-1}}$ (by Lemma 14) imply $M_p | v_{2^{p-1}}$)) equal $M_p$ (by Lemma 15 (f), i.e., $M_p$ is itself a prime. Q. E. D.
The question naturally arises, "Why that particular series?", i.e., 4, 14, 196, ... . Lehmer goes on to show (Lehmer 1935) that $S_1 = 4$ is one of only $2^{P-2}$ different numbers mod $M_p$ available for conducting a Lucas-Lehmer test for $M_p$.

These $2^{P-2}$ different $S_{1,i}$ are determined by the relationship

$$S_{1,i+1} = 14S_{1,i} - S_{1,i-1}$$

where $S_{1,1} = 4$ and $S_{1,2} = 52$ (Kravitz 1970).

Thus, in determining the primality of $2^P - 1$ where $p = 7$, we can initialize our Lucas' sequence with not only 4 or 52, but with 30 other numbers, mod 127. Kravitz (1970) demonstrates how each of the 32 cases for $p = 7$ converge to 0 at $S_6$:
Since World War II, any serious attempt to discover new perfect numbers has had to make use of implementing the Lucas-Lehmer Theorem on a computer. With this in mind, it appears that as a general rule, new additions to the list of perfect numbers will come from those individuals who can code the Lucas-Lehmer Theorem efficiently, and who have significant periods of idle time available to them (processor idle time, that is!).

Of great help in increasing one's chances of discovering new perfect numbers is knowing what numbers to skip. Several lists of Mersenne numbers which have known prime factors have been generated. Among the most used is that generated by Wagstaff (unpublished, but available from him), D. H. Lehmer (1947), A. J. C. Cunningham and H. J. Woodall (1925), and M. Kraitchik (1938). Some simple lists can be easily generated. Euler, for example, noted that if \( n = 4m - 1 \) and \( 8m - 1 \) are both primes, then \( 8m - 1 \) divides \( 2^n - 1 \) (Dickson 1971). Theorem 8 is equivalent.

**Theorem 8:** If \( q = 2p + 1 \) is a prime, where \( p = 4k + 3 \) is also a prime, for \( k > 0 \), then \( q | M_p \), that is, \( q | 2^p - 1 \).

**Proof:** The case where \( k = 2 \) is obvious ..., \( p = 11 \), \( q = 23 \) and \( M_{11} = 2047 = 23 \cdot 89 \).
Otherwise, let $p$ be an odd prime. $p$ must be of the form $4k + 1$ or $4k + 3$. If $p$ is of the form $4k + 3$, then $q$ must be of the form $2(4k + 3) + 1$, or $8k + 7$. Similarly, if $p$ is of the form $4k + 1$, then $q$ must be of the form $2(4k + 1)$, or $8k + 3$.

The result follows immediately from Lemma 10.

**EXAMPLES:**

<table>
<thead>
<tr>
<th>$k$</th>
<th>$p$</th>
<th>$q$</th>
<th>thus</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>11</td>
<td>23</td>
<td>$23</td>
</tr>
<tr>
<td>5</td>
<td>23</td>
<td>47</td>
<td>$47</td>
</tr>
<tr>
<td>20</td>
<td>83</td>
<td>167</td>
<td>$167</td>
</tr>
<tr>
<td>32</td>
<td>131</td>
<td>263</td>
<td>$263</td>
</tr>
<tr>
<td>44</td>
<td>179</td>
<td>359</td>
<td>$359</td>
</tr>
<tr>
<td>47</td>
<td>191</td>
<td>383</td>
<td>$383</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>etc.</td>
</tr>
</tbody>
</table>

Besides obtaining or generating lists of Mersenne numbers with known factors, much time can be saved by knowing where to check on the results of others.

Fortunately, this is not too difficult as the number of serious researchers is few and most tend to get any new material published in the journal *Mathematics of Computation*. Following is a brief summary of post-World War II work by the people who made the most notable contributions.

**HORACE UHLER AND CHARLES B. BARKER**

Yale University professor H. S. Uhler was perhaps the last to make significant contributions in perfect numbers by hand methods. By the mid-1940's the character of all Mersenne numbers less than or equal
to $p = 257$ had been established except for $p = 157, 167, 199, 227$ and 229. Uhler tried Powers' method (Power 1934) but gave up after the 34th step of Lucas's sequence. He remarked that "it had proved to involve an inordinate amount of writing and mental arithmetic and especially because it did not make use of a computing machine exclusively" (Uhler 1944). Uhler's method, a slight modification that allowed him to multiply by a reciprocal of a number, allowed him to continue, apparently unperturbed by the amount of writing involved. Uhler's method is described in detail in the previously mentioned reference.

On August 11, 1944, Uhler determined the 156th residue of Lucas' sequence mod $M_{157}$, a non-zero number, hence $M_{157}$ was composite.

Four months later, on December 11, 1944, Charles B. Barker of the University of New Mexico announced that he too had determined a new Mersenne composite, $M_{167}$ (Barker 1945). Barker used an "eight-bank electric calculating machine" as he called it, and checked each of his residues, $r_{i-1}$, by comparing them with his computation of $(M_{167} - r_{i-1})^2 - 2$. Barker also had independently confirmed Uhler's calculation of $r_{156}$ (mod 157) as he discovered in later correspondence between the two men. Barker learned that Uhler had discovered the factorability of $M_{167}$ nine days before. In fact, Uhler want on to determine the factorability of the other four "unknown" Mersenne numbers; $M_{193}$ (November 27, 1947), $M_{199}$ (July 27, 1946), $M_{227}$ (June 4, 1947) and $M_{229}$ (February 9, 1946) (Uhler 1948).

A. M. TURING

A. M. Turing of the University of Manchester deserves a brief mention here as, in 1951, he was the first to use an electronic com-
puter in the search for Mersenne primes. He didn't find any. Whether out of disgust, lack of interest or what, it appears that Turing discarded his computed residues, as I cannot find any article that used Turing's work as a reference.

D. H. LEHMER AND RAPHAEL ROBINSON

D. H. Lehmer, whose contributions to the topic were already well noted, and his colleague at Berkeley, Raphael M. Robinson, were the first to be successful in the search for perfect numbers with the use of an electronic computer. They used the computer referred to as the National Bureau of Standards' Western Automatic Computer (SWAC, for short) at the Institute of Numerical Analysis in California in 1952. Lehmer, his wife Emma, and others in the Institute helped support the work of Robinson, who evidently was the driving force behind the project as he is generally given credit for their successes (he did the coding).

On January 30, 1952 the program was tried for the first time and resulted in the discovery of two new Mersenne primes, $M_{521}$ and $M_{607}$, the first discoveries since 1914 (Lehmer 1952). The I. N. A. team tested all $p < 2304$ at least twice, discovering three more primes in the process: $M_{1279}$ (June 25, 1952, 13 min. 25 sec. CPU time); $M_{2203}$ (October 7, 1952) and $M_{2281}$ (October 9, 1952). The latter two computations took 59 and 66 minutes respectively (Uhler 1953).

This work was also significant in that it provided the first opportunity to check the manual work of many of their predecessors by automatic methods. Much to their delight, most established results were corroborated, especially that of Uhler and Lehmer (Robinson 1954).
On the other hand, Barker's residue for $M_{167}$ was shown to be incorrect, as were Fauquembergue's residues for $p = 101, 103, 109$ and 137.

HANS RIESEL

Hans Riesel received some time on the Swedish computer BESK during 1957. Riesel writes, "The intention of the author's investigation on the BESK was to check some known results, and to examine some Mersenne numbers not previously examined." (Riesel 1958)

In order to test his program, Riesel corroborated the 17 known perfect numbers. Riesel continued the exploration of $p > 2300$, to pick up where Robinson left off. To save a little time, since each run took several hours, Riesel generated a list of factors of $2^p - 1$ for all $p < 1000$ that followed the guidelines of Theorems 5 and 6, i.e., if $q$ is a factor of $M_p$, then $q = 2kp + 1$ and $q = 8s + 1$. Riesel calculated all such factors less than 10,485,760 and determined to which $M_p$ they belonged, if any, for $p < 10000$. (Riesel 1958)

With this table in hand, Riesel proceeded to extend the upper bound of "known $p"", stopping at $p = 3300$. On September 18, 1957, he found the only Mersenne prime in the range $2300 < p < 3300$, $M_{3217}$, which required 5 hours and 30 minutes of CPU time. (Riesel 1958)

Riesel later published much larger tables. (Riesel 1962) In addition to the work of J. Brillhart and G. D. Johnson (1960), among others, Riesel helped examine all $p < 10000$ by 1962.

J. L. SELFRIDGE AND ALEXANDER HURWITZ

Alexander Hurwitz of U. C. L. A. extended the upper limit of "known $p"" to 5000, noting two new primes, $M_{4253}$ and $M_{4423}$ (both on November 1, 1963). (Hurwitz 1962) Hurwitz used his university's IBM
7090. An indication of the lack of reliability of electronic computers, even at this seemingly late date, was Hurwitz's program's tendency for an "occasional" error. Hurwitz originally wrote his program merely to demonstrate its use on M\textsuperscript{13}. At least four errors occurred in production runs before the same result was obtained twice! (Selfridge and Hurwitz 1964) To detect errors as they occurred, Selfridge and Hurwitz computed each product and each reduction by a different modulus, 2\textsuperscript{35} - 1, and compared results. This allowed them to determine the "probable" answer before proceeding. All serious researchers since have incorporated similar checks in their programs, dependent for the most part on their coding and the limits of the hardware, operating system and programming language used.

Hurwitz continued to search for new primes for 5000 < p < 6000, without success.

SIDNEY KRAVITZ AND MURRAY BERG

Kravitz and Berg, of Standard Oil of California, tested 6000 < p < 7000 with no new results.

DONALD B. GILLIES

Gillies, of the Digital Computer Laboratory at the University of Illinois, offered what was probably the first significant theoretical contribution to the subject of perfect numbers since D. H. Lehmer's "An Extended Theory of Lucas' Function" established the Lucas-Lehmer Theorem.

Gillies discovered three new Mersenne primes while using the Illiac II at the Digital Computer Laboratory; M\textsuperscript{9689}, M\textsuperscript{9941} and M\textsuperscript{11213}, which took 1 hour 23 minutes, 1 hour 30 minutes and 2 hours 15 minutes
of CPU time respectively. (Gillies 1964) Gillies continued searching all \( p < 12000 \) for which no previous research was known.

Gillies' work was also evidence to the increasing power of electronic computers. Gillies writes, "the residue of \( M_{8191} \) took 100 hours on Illiac I (D. J. Wheeler), 5.2 hours on an IBM 7090 (Hurwitz 1962), and 49 minutes on Illiac II." (Gillies 1964)

The relatively large gap that Gillies noted between \( M_{4423} \) and \( M_{9689} \) brought forth questions concerning the distribution of Mersenne primes. In his article "Three New Mersenne Primes and a Statistical Theory" (Gillies 1964), he tries to improve the conjectures of I. J. Good (Good 1955) who believed that the number of Mersenne primes less than \( x \) was asymptotic to \( 2.3 \log \log x \); and Daniel Shanks (Shanks 1962) who suggested that \( 5/\log 10 \log \log x \) was the better estimate.

Gillies' conjecture is as follows:

\[
A < B \leq \sqrt{M_p}, \text{ as } B/A \text{ and } M_p \text{ tend towards infinity,}
\]

the number of prime divisors of \( M_p \) in the interval \( (A,B) \) is Poisson distributed with mean \( \sim \log (\log B/\log A) \) if \( A > 2p \)

or \( \sim \log (\log B/\log 2p) \) if \( A < 2p \).

If true, this conjecture implies that

1. the number of Mersenne primes less than \( x \) is \( (2/\log 2) \log \log x \),
2. the expected number of Mersenne primes in the interval \([x,2x]\) in \( p \) is \( 2 + 2 \log[\log 2x/\log x] \),
3. the probability that \( M_p \) is prime is

\[
\sim (2 \log 2p)/(p \log 2).
\]

(Gillies 1964)

Of perhaps greater interest, at least at first, is the Eberhart Conjecture (Slowinski 1979) that the \( i^{th} \) Mersenne prime lies near \( (3/2)^i \). This conjecture follows very closely to the pattern of known
Mersenne primes, much more so than any of the conjectures just mentioned, but that is no reason to conclude the same for its asymptotic behavior.

BRYANT TUCKERMAN

Bryant Tuckerman, an employee of the IBM Thomas J. Watson Research Center in Yorktown Heights, New York, probably represents the beginning of the users of what we could call "modern" computers, if one does not want to give that distinction to Hurwitz or Gillies. While Gillies took pride in computing the residue of $M_{8191}$ in 49 minutes, Tuckerman's IBM 360/91 took 3.17 minutes. With his greater computing punch, Tuckerman was able to extend the upper limit of "known p" to 21,000, discovering the primality of the 24th Mersenne prime, $M_{19937}$ (March 4, 1971). (Tuckerman 1971).

Bryant Tuckerman's article demonstrated the squaring algorithm used by himself, by Nickel and Noll, and no doubt by others:

$$u^2 = \sum_{k=0}^{L-1} x_k^2 B^k + \sum_{k=1}^{2L-3} B^{2k-2} \sum x_i x_j,$$

where the right-most summation runs over all $(i, j)$ such that $i + j = k$ and $0 \leq i \leq j \leq L - 1$, with appropriate provisions for carries, unpacking partial results, etc.

(Tuckerman 1971)

From this point of view, it is easy to see the speed of the Lucas-Lehmer Theorem is still dependent on the speed of squaring the numbers in the Lucas's sequence; for the mod $M_p$ reduction, as demonstrated previously, is merely a bit shift and requires no computation at all. Thus, to multiply two at-most-p-bits numbers, we would require at most $p^2$ multiplications. Since our Lucas's sequence must be carried
to the $p^{-1\text{st}}$ term, we see that this application is of order $p^3 - p$, or simply of order $p^3$.

LAURA NICKEL AND CURT NOLL

Laura Nickel and Curt Noll made the CBS Evening News in 1979 not so much for discovering a new Mersenne prime, but for the fact that they were not mathematics professors or computer scientists, but a couple of ambitious students barely out of high school.

Using the CDC Cyber 174 at the University of California at Hayward, Nickel and Noll extended Tuckerman's work and discovered, on October 30, 1978, that $M_{21701}$ was prime. (Nickel and Noll 1980) Noll made modifications to the program and continued on to test all $p < 24500$, discovering the primality of $M_{23209}$ on February 9, 1979, using 8 hours, 39 minutes and 37 seconds of CPU time.

While four other Mersenne primes have been discovered since (see Slowinski next), Curt Noll's Mersenne prime remains the last discovered by a systematic search of all $p$ greater than the upper bound of "known $p$". Steve McGrogan, a systems analyst at Elxsi Computer in San Jose, California, has worked to extend this upper limit, but has so far announced no new discoveries.

DAVID SLOWINSKI

David Slowinski, credited with writing the program that has discovered the last four Mersenne primes, is in the enviable position of being an employee of the Cray Research firm in Chippewa Falls, Wisconsin, thus having access to the state of the art Cray computers. As an example of the tremendous advantage that the Cray-1 had over its competition (please bear in mind that the Cray-1 is now an out-
dated model), the $M_{8191}$ residue calculation previously mentioned as having taken 3.17 minutes on an IBM 360 (no slouch in computing power), took a mere 10 seconds by Slowinski's program.

Slowinski, like others before him, eliminated many potential $M_p$ by consulting Wagstaff's table. Several modifications were made to his program by colleague Harry Nelson which greatly reduced the computation time required.

In a conversation that I had with Slowinski in January of 1986, he tactfully side-stepped any questions concerning the contents of his coding, but readily admitted to having incorporated the Schonhage-Strassen Fast-Fourier Multiplication method, as described in Donald Knuth's The Art of Computer Programming (1982), Vol. 2, which increases computational speed from order $p^3$ to order $(n \log n \log \log n)$. (Knuth 1982)

The Knuth reference appears to be indespensible to anybody who wishes to write a competitive program for finding Mersenne primes. Improvements shouldn't stop here, however, as Schonhage notes, in the same reference, that multiplication of very large numbers appears to be practical on the order of order $n$, as difficult as that may seem to believe. No one as yet appears to have succeeded.

Slowinski hasn't been systematical in his search for more Mersenne primes, byt rather takes occasional stabs in the dark when given the opportunity to confidence test a new Cray installation. Still, he has four new primes to his credit: $M_{44497}$ (April 8, 1979), $M_{86243}$ (1982), $M_{132049}$ (1983) and $M_{216091}$ (September, 1985). (Personal correspondence)
As has been mentioned before, the name of the game is speed, hence the success of Cray. Any program of note, to increase its computation speed, should be written in an assembler language, usually working with binary numbers, although other bases have been tried. The use of multiple-precision numbers also allows the amount of work necessary to handle crossing word boundaries to be minimized.

Current competition also dictates that more efficient coding be implemented for the squaring routine. The old order $p^3$ speed is no longer competitive.

While the author would love dearly to write a competitive program for finding perfect numbers, my knowledge of assembler languages is nil, and my grasp of computer programming and computer architecture necessary to handle the Schonhage-Strassen Fast-Fourier Multiplication method is is comparable. This should not stop a person with knowledge of at least one higher-level language from writing a program that works. FORTRAN, for example, usually has some accommodation for reading or manipulating the binary form of a number. One manufacturer uses the ISHFT(v,m) command, where the bits in the binary form of the number v are shifted m places; to the right, if m is positive; to the left if m is negative. Another installation allows you to read the bits in a word and assign them to another variable. Hence, $J = \text{FLD}(m,n,v)$ reads the binary representation of the number v, starting at bit number m, for n bits, and assigns the determined value to the variable J.
In Appendix C of this paper is a simple program written in the WATFIV version of FORTRAN that will determine the primality of Mersenne numbers. While Slowinski can sleep soundly tonight, the program is capable of determining the primality of at least the first few hundred Mersenne numbers. How far it will reach depends on the memory allowed by the installation on which it is implemented.

DESCRIPTION OF THE PROGRAM

* Each residue is divided into 18-bit words, hence the largest number that can be accomodated by a single word is $2^{18} - 1$.

* The number is squared word-by-word, much as one would perform the long-hand multiplication, giving us $[p/18]$ rows of $[p/18]$ words.

* This particular installation uses 36 bit words, however the FLD command is limited to this range, hence no attempt is made to use double precision. In each row of partial products, any number found in bits 0 through 17 is carried into the word to its immediate left.

* The partial products are then added by column, giving us a $[p/18] \cdot 2$ bit word.

* Again, any numbers found in bit positions 0 through 17 are carried into the word to its immediate left. Our finished product is at most $[p/18] \cdot 2 + 1$ words long.

* It is determined in which word the break occurs between the low-order $p$ bits and the high-order $p$ bits, wherein the high-order bits of that word are shifted to word (1), and the bits of any words to the left of this word are added to their respective low-order counterparts.
* A check is made to see if a bit has been carried over into the first position of the high-order bits. If so, that '1' is shifted (added) to the far right of the first word on the right.

* If the number's bits are all ones, then we have a Mersenne prime.
APPENDIX A. ON ODD PERFECT NUMBERS

While this paper claims to be on perfect numbers, the absence of any discussion on odd perfect numbers in the paper's body at first appears to be a glaring omission. I offer no apologies, however. The paper concerns looking for perfect numbers, and it seems only fitting that one should stroll down the only road that has produced any discoveries.

It appears highly unlikely that any progress towards proving or disproving the existence of odd perfect numbers is imminent. Work on odd perfect numbers continues to fall into two general categories:

1) showing what form they or their factors must take, and
2) showing how large the first one is, or how large one of its factors must be.

Concern for odd perfect numbers evidently wasn't of much concern until the time of Euler, who proved that any odd perfect number must be of the form \( r^{4m+1} p^2 \), where \( r \) is a prime of the form \( 4n + 1 \). (Dickson 1971) He also showed that no odd perfect number can be of the form \( 4n + 3 \). Euler later showed that if \( n \) is an odd perfect number, then

\[
n = p^a q_1^{2b_1} q_2^{2b_2} q_3^{2b_3} \ldots q_t^{2b_t},
\]
where \( p, q_1, q_2, \ldots, q_t \) are distinct odd primes and \( a = 1 \equiv p \pmod{4} \). (McCarthy 1957)

There have been many contributions to the question of form and size of odd perfect numbers in recent years, most notably by Peter Hagis, Jr., Wayne McDaniel and Carl Pomerance, the last of whom wrote one of only three or four known Ph. D. dissertations on perfect numbers (all of which are on odd perfect numbers). (Pomerance 1974)

Hagis and McDaniel showed that if \( n \) is odd and perfect, then \( n \) has a prime divisor larger than 11,200; that no odd perfect number exists below \( 10^{50} \); and other results. Discussing each of these, even briefly, would take up considerable space, but would not help you find perfect numbers.

The interested reader who would like to know more about odd perfect numbers would do well by checking the articles by Hagis, McDaniel and McCarthy listed in the references.
APPENDIX B. THE THIRTY KNOWN MERSENNE PRIMES

<table>
<thead>
<tr>
<th>PRIME</th>
<th>DISCOVERER</th>
<th>DATE</th>
<th>METHOD</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. 2</td>
<td>ancient</td>
<td>---</td>
<td>hand</td>
</tr>
<tr>
<td>2. 3</td>
<td>ancient</td>
<td>---</td>
<td>hand</td>
</tr>
<tr>
<td>3. 5</td>
<td>ancient</td>
<td>---</td>
<td>hand</td>
</tr>
<tr>
<td>4. 7</td>
<td>ancient</td>
<td>---</td>
<td>hand</td>
</tr>
<tr>
<td>5. 13</td>
<td>unknown</td>
<td>&lt; 1456</td>
<td>hand</td>
</tr>
<tr>
<td>6. 17</td>
<td>Cataldi</td>
<td>1588</td>
<td>division by primes ( &lt; \sqrt{p} )</td>
</tr>
<tr>
<td>7. 19</td>
<td>Cataldi</td>
<td>1588</td>
<td>division by primes ( &lt; \sqrt{p} )</td>
</tr>
<tr>
<td>8. 31</td>
<td>Euler</td>
<td>1772</td>
<td>Division by primes ( &lt; \sqrt{p} ) of the form ( 2kp + 1 ) and ( 8j + 1 )</td>
</tr>
<tr>
<td>9. 61</td>
<td>Pervusin</td>
<td>1883</td>
<td>Lucas Test</td>
</tr>
<tr>
<td></td>
<td>Seelhoff</td>
<td>1886</td>
<td>Lucas Test</td>
</tr>
<tr>
<td>10. 89</td>
<td>Powers</td>
<td>1911</td>
<td>Lucas Test</td>
</tr>
<tr>
<td></td>
<td>Fauquembergue</td>
<td>1912</td>
<td>Lucas Test</td>
</tr>
<tr>
<td>11. 107</td>
<td>Fauquembergue</td>
<td>1914</td>
<td>Lucas Test</td>
</tr>
<tr>
<td></td>
<td>Powers</td>
<td>1914</td>
<td>Lucas Test</td>
</tr>
<tr>
<td>12. 127</td>
<td>Lucas</td>
<td>1876</td>
<td>Lucas Test</td>
</tr>
<tr>
<td>13. 521</td>
<td>Robinson, Lehmer</td>
<td>1952</td>
<td>Lucas Test - SWAC</td>
</tr>
<tr>
<td>14. 607</td>
<td>Robinson, Lehmer</td>
<td>1952</td>
<td>Lucas Test - SWAC</td>
</tr>
<tr>
<td>15. 1279</td>
<td>Robinson, Lehmer</td>
<td>1952</td>
<td>Lucas Test - SWAC</td>
</tr>
<tr>
<td>PRIME</td>
<td>DISCOVERER</td>
<td>DATE</td>
<td>METHOD</td>
</tr>
<tr>
<td>---------</td>
<td>-----------------------</td>
<td>--------</td>
<td>-------------------------------</td>
</tr>
<tr>
<td>16. 2203</td>
<td>Robinson, Lehmer</td>
<td>1952</td>
<td>Lucas Test - SWAC</td>
</tr>
<tr>
<td>17. 2281</td>
<td>Robinson, Lehmer</td>
<td>1952</td>
<td>Lucas Test - SWAC</td>
</tr>
<tr>
<td>18. 3217</td>
<td>Riesel</td>
<td>1957</td>
<td>Lucas Test - BESK</td>
</tr>
<tr>
<td>19. 4253</td>
<td>Hurwitz, Selfridge</td>
<td>1961</td>
<td>Lucas-Lehmer Test - IBM 7090</td>
</tr>
<tr>
<td>20. 4423</td>
<td>Hurwitz, Selfridge</td>
<td>1961</td>
<td>Lucas-Lehmer Test - IBM 7090</td>
</tr>
<tr>
<td>21. 9689</td>
<td>Gillies</td>
<td>1963</td>
<td>Lucas-Lehmer Test - Illiac II</td>
</tr>
<tr>
<td>22. 9941</td>
<td>Gillies</td>
<td>1963</td>
<td>Lucas-Lehmer Test - Illiac II</td>
</tr>
<tr>
<td>23. 11213</td>
<td>Gillies</td>
<td>1963</td>
<td>Lucas-Lehmer Test - Illiac II</td>
</tr>
<tr>
<td>24. 19937</td>
<td>Tuckerman</td>
<td>1971</td>
<td>Lucas-Lehmer Test - IBM 360/91</td>
</tr>
<tr>
<td>25. 21701</td>
<td>Nickel, Noll</td>
<td>1978</td>
<td>Lucas-Lehmer Test - CDC Cyber 174</td>
</tr>
<tr>
<td>26. 23209</td>
<td>Noll</td>
<td>1979</td>
<td>Lucas-Lehmer Test - CDC Cyber 174</td>
</tr>
<tr>
<td>27. 44497</td>
<td>Slowinski</td>
<td>1979</td>
<td>Lucas-Lehmer Test - Cray-1 S/N 10</td>
</tr>
<tr>
<td>28. 86243</td>
<td>Slowinski</td>
<td>1982</td>
<td>Lucas-Lehmer Test - Cray-1</td>
</tr>
<tr>
<td>29. 132049</td>
<td>Slowinski</td>
<td>1983</td>
<td>Lucas-Lehmer Test - Cray X-MP/24</td>
</tr>
<tr>
<td>30. 216091</td>
<td>Slowinski</td>
<td>1985</td>
<td>Lucas-Lehmer Test - Cray X-MP/24</td>
</tr>
</tbody>
</table>
APPENDIX C. COMPUTER PROGRAM

LIST

10 IMPLICIT INTEGER (A-Z)
20 DIMENSION WORD(13),STORE(9,8)
30 PRIME=31
40 WORD(1)=4
50 WORDCT=1
60 WRDCT1=1
70 WRITE(6,70)
80 70 FORMAT('0','START PASS NO. 1')
90 WRITE(6,80) 4
100 80 FORMAT(' RESIDUE WORD(1)= ','20X','*** ','I6',' ***')
110C
120C THIS LOOP SQUARES U(N) AND STORES IT IN 'STORE'
130C
140 DO 1537 PASS=2,PRIME-1
150 WRITE(6,130) PASS
160 130 FORMAT('0','START PASS NO. ',I2)
170   DO 200 CTROW=1,WORDCT
180     DO 170 CTCOL=1,WORDCT
190       STORE(CTROW,CTROW-1+CTCOL)=WORD(CTROW)*WORD(CTCOL)
200   170 CONTINUE
210 200 CONTINUE
220C
230C THIS LOOP CARRIES ANY CHARACTERS IN BIT POSITIONS 0-17
240C INTO THE NEXT WORD TO ITS IMMEDIATE LEFT AND DETERMINES
250C HOW MANY WORDS IT TAKES UP
260C
270 WRDCT1=WORDCT*2-1
280 DO 330 CTROW=1,WORDCT
290   DO 325 CTCOL=1,WORDCT
300     J=FLD(0,18,STORE(CTROW,CTROW-1+CTCOL))
310     IF (J.EQ.0) GOTO 325
320     WRDCT1=MAX0(WRDCT1,CTROW+CTCOL)
330   325 STORE(CTROW,CTROW+CTCOL)=STORE(CTROW,CTROW+CTCOL)+J
340   330 STORE(CTROW,(CTROW-1)+CTCOL)=FLD(18,18,STORE(CTROW,(CTROW-1)+CTCOL))
CONTINUE
360 330 CONTINUE
370C
380C THIS LOOP ADDS UP THE FIRST WORDCT COLUMNS
390C
400 DO 420 CTCOL=1,WORDCT
410 DO 415 CTROW=1,CTCOL
420 STORE(WORDCT+1,CTCOL)=STORE(WORDCT+1,CTCOL)+STORE(CTROW,CTCOL)
430 415 CONTINUE
440 420 CONTINUE
450C
460C THIS LOOP ADDS UP THE REMAINING COLUMNS
470C
480 IF (WRDCT1.EQ.WORDCT) GOTO 550
490 DO 500 CTCOL=WORDCT+1,WRDCT1
500 DO 490 CTROW=CTCOL-WORDCT,WORDCT
510 490 STORE(WORDCT+1,CTCOL)=STORE(WORDCT+1,CTCOL)+STORE(CTROW,CTCOL)
520 500 CONTINUE
530C
540C THIS LOOP CARRIES ANY CHARACTERS IN THE PRODUCT IN BIT
550C POSITIONS 0-17 INTO THE NEXT WORD TO ITS IMMEDIATE LEFT
560C
570 550 DO 600 CTCOL=1,WRDCT1
580 J=FLD(0,18,STORE(WORDCT+1,CTCOL))
590 IF (J.EQ.0) GOTO 600
600 STORE(WORDCT+1,CTCOL+1)=STORE(WORDCT+1,CTCOL+1)+J
610 STORE(WORDCT+1,CTCOL)=FLD(18,18,STORE(WORDCT+1,CTCOL))
620 600 CONTINUE
630C
640C THIS LOOP RESETS WORD TO ALL ZEROES
650C
660 DO 650 CTCOL=1,WRDCT1
670 650 WORD(CTCOL)=0
680C
690C SUBTRACTING ROUTINE
700C
710 IF (STORE(WORDCT+1,1).LT.2) GOTO 890
720 850 STORE(WORDCT+1,1)=STORE(WORDCT+1,1)-2
730 GOTO 1090
740 890 IF (STORE(WORDCT+1,2).EQ.0) GOTO 950
750 STORE(WORDCT+1,2)=STORE(WORDCT+1,2)-1
760 STORE(WORDCT+1,1)=STORE(WORDCT+1,1)+2**18
770 GOTO 850
780C
790C THIS LOOP DETERMINES IF THERE'S ANYTHING TO BORROW FROM
800C
810 950 DO 990 I=3,WORDCT1
820 IF (STORE(WORDCT+1,I).GT.0) GOTO 1050
830 990 CONTINUE
840C
850C BORROWING ROUTINE
860C
870 1050 DO 1060 J=2,I-1
880 1060 WORD(J)=2**18-1
890 WORD(I)=WORD(I)-1
900 WORD(I)=2**18-2
910C
920C BIT SHIFTING ROUTINE FOR BREAK WORD
930C
940 1090 BREAK=PRIME/18+1
950 HIGHSZ=18-(PRIME-(PRIME/18)*18)
960 TRANS=FLD(0,18+HIGHSZ,STORE(WORDCT+1,BREAK))
970 WORD(1)=STORE(WORDCT+1,1)
980 IF (TRANS.NE.0) GOTO 1160
990 WORD(BREAK)=STORE(WORDCT+1,BREAK)
1000 GOTO 1250
1010 1160 WORD(BREAK)=FLD(18+HIGHSZ,18-HIGHSZ,STORE(WORDCT+1,BREAK))
1020 WORD(1)=WORD(1)+TRANS
1030 IF (BREAK.EQ.1) GOTO 1230
1040 WORD(BREAK)=STORE(WORDCT+1,BREAK)-TRANS*(2**(18-HIGHSZ))
1050C
1060C THIS LOOP DOES THE BIT SHIFT ADDITION FOR THE OTHER WORDS
1070C
1080 1230 CONTINUE
1090 1250 IF (WRDCT1.LE.BREAK) GOTO 1305
1100 DO 1300 I=BREAK+1,WRDCT1
1110 TRANS=FLD(18+HIGHSZ,18-HIGHSZ,STORE(WRDCT+1,I))
1120 WORD(I-BREAK)=WORD(I-BREAK)+TRANS*2**HIGHSZ
1130 TRANS=FLD(0,18-HIGHSZ,STORE(WRDCT+1,I))
1140 WORD((I-BREAK)+1)=WORD((I-BREAK)+1)+TRANS
1150 1300 CONTINUE
1160C
1170C THIS LOOP CARRIES ANY CHARACTERS IN BIT
1180C POSITIONS 0-17 INTO THE WORD TO ITS IMMEDIATE LEFT
1190C
1200C
1210 1305 DO 1322 I=1,BREAK
1220 J=FLD(0,18,WORD(I))
1230 IF (J.EQ.0) GOTO 1322
1240 WORD(I+1)=WORD(I+1)+J
1250 WORD(I)=FLD(18,18,WORD(I))
1260 1322 CONTINUE
1270 1335 OVER=FLD(17+HIGHSZ,1,WORD(BREAK))
1280 IF (OVER.EQ.0) GOTO 1355
1290 WORD(1)=WORD(1)+1
1300 WORD(BREAK)=FLD(18+HIGHSZ,36-(18+HIGHSZ),WORD(BREAK))
1310C
1320C THIS LOOP DETERMINES HOW MANY WORDS ARE NECESSARY TO REPRESENT OUR NEW PRODUCT
1330C
1340C
1350 1355 IF (BREAK.NE.1) GOTO 1359
1360 WRDCT1=1
1370 GOTO 1390
1380 1359 WRDCT1=BREAK
1390 DO 1375 CTCOL=1,BREAK
140 IF (WORD(BREAK+1-CTCOL).NE.0) GOTO 1390
141 WRDCT1=WRDCT1-1
142 1375 CONTINUE
1430C
1440C THIS LOOP WRITES OUR RESIDUE
1450C
1460 1390 DO 1420 I=1,WRDCT1
1470 WRITE(6,1410) I,WORD(I)
1480 1410 FORMAT(1X,'RESIDUE WORD(','I2,')='20X,'*** ','I6, '***')
1490 1420 CONTINUE
1500C
1510C THIS LOOP RESETS THE VALUES OF 'STORE' TO ZERO
1520C
1530 DO 1490 CTROW=1,WORDCT+1
1540 DO 1480 CTCOL=CTROW,WORDCT*2+1
1550 STORE(CTROW,CTCOL)=0
1560 STORE(WORDCT+1,CTROW)=0
1570 STORE(CTCOL,CTROW)=0
1580 1480 CONTINUE
1590 1490 CONTINUE
1600 WORDCT=WRDCT1
1610 1537 CONTINUE
1620C
1630C THIS LOOP DETERMINES IF OUR RESIDUE IS EQUAL TO 0 (MOD P)
1640C
1650 IF (WORD(PRIME/18+1).NE.(2**(PRIME-(PRIME/18)*18)-1)) GOTO 1690
1660 IF ((PRIME/18+1).EQ.1) GOTO 1590
1670 DO 1580 I=1,PRIME/18
1680 IF (WORD(I).NE.2**18-1) GOTO 1690
1690 1580 CONTINUE
1700 1590 WRITE(6,1600) PRIME
1710 1600 FORMAT(1X,'CONGRATULATIONS!!!','I8,' IS A MERSENNE PRIME!')
1720 GOTO 1710
1730 1690 WRITE(6,1700) PRIME
1740 1700 FORMAT('0','SORRY. ','I3,' IS A MERSENNE COMPOSITE.')
1750 1710 STOP
1760 END

>30 PRIME=3
>FRN
START PASS NO. 1
RESIDUE WORD(1)= *** 4 ***
START PASS NO. 2
RESIDUE WORD( 1)= *** 7 ***
CONGRATULATIONS!!! 3 IS A MERSENNE PRIME!

>30 PRIME=5
>FRN
START PASS NO. 1
RESIDUE WORD(1)= *** 4 ***
START PASS NO. 2
RESIDUE WORD( 1)= *** 14 ***
START PASS NO. 3
RESIDUE WORD( 1)= *** 8 ***
START PASS NO. 4
RESIDUE WORD( 1)= *** 31 ***
CONGRATULATIONS!!! 5 IS A MERSENNE PRIME!

>30 PRIME=7
>FRN
START PASS NO. 1
RESIDUE WORD(1)= *** 4 ***
START PASS NO. 2
RESIDUE WORD( 1)= *** 14 ***
START PASS NO. 3
RESIDUE WORD( 1)= *** 67 ***
START PASS NO. 4
RESIDUE WORD( 1)= *** 42 ***
START PASS NO. 5
RESIDUE WORD( 1)= *** 111 ***
START PASS NO. 6
RESIDUE WORD(1) = *** 127 ***
CONGRATULATIONS!!! 7 IS A MERSENNE PRIME!

>3Ø PRIME=11
>FRN
START PASS NO. 1
RESIDUE WORD(1) = *** 4 ***
START PASS NO. 2
RESIDUE WORD(1) = *** 14 ***
START PASS NO. 3
RESIDUE WORD(1) = *** 194 ***
START PASS NO. 4
RESIDUE WORD(1) = *** 788 ***
START PASS NO. 5
RESIDUE WORD(1) = *** 7P1 ***
START PASS NO. 6
RESIDUE WORD(1) = *** 119 ***
START PASS NO. 7
RESIDUE WORD(1) = *** 1877 ***
START PASS NO. 8
RESIDUE WORD(1) = *** 240 ***
START PASS NO. 9
RESIDUE WORD(1) = *** 282 ***
START PASS NO. 10
RESIDUE WORD(1) = *** 1736 ***
SORRY. 11 IS A MERSENNE COMPOSITE.

>3Ø PRIME=13
>FRN
START PASS NO. 1
RESIDUE WORD(1) = *** 4 ***
CONGRATULATIONS!!! 13 IS A MERSENNE PRIME!

>30 PRIME=17
>FRN

START PASS NO. 1
RESIDUE WORD(1)= *** 4 ***
START PASS NO. 2
RESIDUE WORD(1)= *** 14 ***
START PASS NO. 3
RESIDUE WORD(1)= *** 194 ***
START PASS NO. 4
RESIDUE WORD(1)= *** 37634 ***
START PASS NO. 5
RESIDUE WORD(1)= *** 95799 ***
START PASS NO. 6
RESIDUE WORD(1)= *** 119121 ***
START PASS NO. 7
RESIDUE WORD(1)= *** 66179 ***
START PASS NO. 8
RESIDUE WORD( 1)=
START PASS NO. 9
RESIDUE WORD( 1)=
START PASS NO. 10
RESIDUE WORD( 1)=
START PASS NO. 11
RESIDUE WORD( 1)=
START PASS NO. 12
RESIDUE WORD( 1)=
START PASS NO. 13
RESIDUE WORD( 1)=
START PASS NO. 14
RESIDUE WORD( 1)=
START PASS NO. 15
RESIDUE WORD( 1)=
START PASS NO. 16
RESIDUE WORD( 1)=
CONGRATULATIONS!!!

17 IS A MERSENNE PRIME!
REFERENCES

Brauer, Alfred. "Note on the Non-existence of Odd Perfect Numbers of Form $p^2q_1^2q_2^2...q_{t-1}^2q_t^4$." Bulletin of the American Mathematical Society 49 (1943):937.
Brauer, Alfred. "On the Non-existence of Odd Perfect Numbers of Form $p^2q_1^2q_2^2...q_{t-1}^2q_t^4$." Bulletin of the American Mathematical Society 49 (1943):712-718.
Brillhart, John D. "H. Riesel, 'All Factors $q < 10^8$ in All Mersenne Numbers $2^p - 1$, $p$, prime $< 10^4$.'" Mathematics of Computation 17 (1963) 215.


Hagis, Peter, Jr. "If $n$ is Odd and Perfect Then $n > 10^{45}$. A Case Study Proof With a Supplement in Which the Lower Bound is Improved to $10^{50}$." (manuscript)


Hagis, Peter, Jr., and McDaniel, Wayne L. "A Proof That Every Odd Perfect Number Has a Prime Factor Greater Than 100100." (manuscript)


Karst, Edgar. "List of All Prime Divisors of \( q = 2kp + 1 \) of \( 2^P - 1 \), \( k < 10 \), \( p < 15000 \)." Nordisk Tidskr. Informations-Behandling 3 (1963):222-228.


Kravitz, Sidney, and Madachy, Joseph S. "Divisors of Mersenne Numbers, 20000 < p < 100000." (manuscript)


McCarthy, Paul J. "The Density of Perfect Numbers." (manuscript)


Noll, Curt L. "Discovering the 26th Mersenne Prime." Dr. Dobb's Journal 4(6) (n.d.):4-5.


Ondrejka, Rudolf. "Mersenne Primes and Perfect Numbers." (manuscript)


Priehipp, Robert W. "Even Perfect Numbers and Seven." Fibonacci Quarterly 6(4) (1968):286.


Selfridge, J. L. "Table Errata." Mathematical Tables and Other Aids To Computation. 13 (1959):142.
Suryanarayana, D. "Inequalities Involving \(\sigma(N), d(N), \varphi(N)\) and Their Application to Odd Perfect Numbers." The Mathematics Student 32 (1964):87-95.
Uhler, Horace S. "The Magnitude of Higher Terms of the Lucasian Sequence 4, 14, 194, ... ." Mathematical Tables and Other Aids to Computation 3 (1948):142-143.
Webber, G. Cuthbert. "Non-existence of Odd Perfect Numbers of the Form $2b_1 a_{s_1} 2b_2 a_{s_2} 2b_3 a_{s_3}$." Duke Mathematics Journal 18 (1967): 741-749.