Some Factorizations of $2^n \pm 1$ and Related Results

By John Brillhart* and J. L. Selfridge*

1. Introduction. In this paper we present a collection of complete factorizations obtained over the past year and a half on the IBM 7090-94 at the UCLA Computing Facility and the Computer Center at the University of California, Berkeley.

The numbers given here are generally of the three forms: $2^n \pm 1$, $2^{2n} \pm 2^n + 1$, and $2^{2n+1} \pm 2^{n+1} + 1$, the latter trinomials occurring naturally in $2^{3n} \mp 1 = (2^n \mp 1)(2^{2n} \pm 2^n + 1)$ and the Aurifeuillian factorization $2^{4n+2} + 1 = (2^{2n+1} - 2^{n+1} + 1)(2^{2n+1} + 2^{n+1} + 1)$. As is customary, we have not removed those algebraic factors of $2^n - 1$ which would produce a quotient more complicated than a trinomial. (As usual, a prime factor of $2^n - 1$ is called "algebraic" if it divides $2^k - 1$ for some $k < n$. Otherwise it is called "primitive".) To distinguish the remaining algebraic factors from the primitive factors, we have given the latter in boldface.

The numbers we have investigated were chosen with an eye to their size, since in general nothing but frustration can be expected to come from an attack on a number of 25 or more digits, even with the speeds available in modern computers. In view of this, factorization (15) is somewhat remarkable.

In the eight factorizations (2), (6), (7), (15), (25), (36), (37), and (39), the new factors were discovered by expressing the composite cofactors as a difference of squares (by "cofactor" we mean the quotient that remains when the known factors are removed). By this means the cofactors were split into pieces that could be identified as primes by either searching for factors up to their square roots, or by testing them for primality. (This method was also used to produce the auxiliary factorizations in (29) and (33).) A brief discussion of the difference of squares method will be given in Section 2.

In the remaining factorizations the completeness was shown by testing their cofactors for primality. The primality tests which were used will be discussed in Section 3.

The paper concludes with a collection of results, which include among others the current status of the numbers $(10^p - 1)/9$, p prime, of the "original" Mersenne numbers, and of the complete factorizations of $2^n \pm 1$.

2. Factorization by a Difference of Squares. (a) The problem of finding factors of a number $N = 2k + 1$ is solved if we can express N as $x^2 - y^2$ in a nontrivial way (by trivial we mean $2k + 1 = (k + 1)^2 - k^2$). The seven factorizations in (2), (6), (7), (15), (29), (37), and (39) were obtained in this way by means of a computer program written by the first author.

This program is based on the familiar exclusion method of Gauss (see Uspensky

Received January 17, 1966. Revised July 18, 1966.

* The preparation of this paper was sponsored by the Office of Naval Research, Contract number Nonr233(76). Reproduction in whole or in part is permitted for any purpose of the United States Government.

and Heaslet [20], Kraitchik [6]) in which the Diophantine equation

$$N = x^2 - y^2 \tag{A}$$

is effectively replaced by the combinatorial problem of solving the set of simultaneous congruences $y^2 \equiv x^2 - N \pmod{E}$ with various "exclusion" moduli E. The requirement that $x^2 - N$ be a quadratic residue for each E places a strong restriction on the values of x. In fact, since each congruence is solvable for only about half of the E values of x for each E, only one x value in 2^s will generally survive the exclusion when s moduli are used.

By experiment it has been found for the IBM 7090 that 21 or 22 moduli are sufficient to sieve out all but a small number of x values, each of which must then be tried in (A). The speed of the sieving program is approximately 150,000 values per second, which is achieved by using 10 or 11 double moduli (such as $E = 17 \cdot 83$) and by operating only at the word level. The method itself is most successful when N can be split into two factors that are close together, as in the auxiliary factorization in (29), where the factors 1061802263 and 1071160627 were discovered in less than a second!

The three factorizations in (25), (33), and (36) were obtained on the new delay-line sieve of D. H. Lehmer at the University of California, Berkeley. This electronic sieve, which became operative on December 1, 1965, is the most recent in a series of remarkable sieving machines that have been built by Professor Lehmer and his associates over the last 40 years (see Lehmer [7], [8], [9], and D. N. Lehmer [16]). The speed of the sieve is 10^6 values per second, a factor of 7 over the speed of the sieving program on the 7090.

(b) When N has a special form, it is often possible to develop modular restrictions on x or y which limit them to a *single* residue class. These restrictions, when they are introduced as a change of variable, considerably reduce the magnitude of the problem when the sieving is carried out on the new variable. For instance, if $N \equiv 2 \pmod 3$, then the congruence $2 \equiv x^2 - y^2 \pmod 3$ implies that $3 \mid x$; for if $x \equiv \pm 1 \pmod 3$, then $y^2 \equiv 2 \pmod 3$, which is impossible. Similarly, if $N \equiv 1 \pmod 3$, then $3 \mid y$.

In the present case where N is a primitive factor of $2^n - 1$ (that is, N is a product of primitive prime factors), we can show that x belongs to a certain arithmetic sequence with a rather large difference. This follows from the known fact that all the factors of N are $\equiv 1 \pmod n$. If $N = (x - y)(x + y)$, we can put $x - y = tn + 1$ and $x + y = un + 1$, which imply

$$N = tun^2 + n(t + u) + 1 \quad \text{and} \quad 2x = n(t + u) + 2. \tag{B}$$

Hence,

$$N = tun^2 + 2x - 1, \quad \text{or} \quad x \equiv \tfrac{1}{2}(N + 1) \pmod{n^2} \quad \text{for } n \text{ odd}, \tag{C}$$

and

$$x \equiv \tfrac{1}{2}(N + 1) \pmod{n^2/2} \quad \text{for } n \text{ even (see Lehmer [10])}. \tag{D}$$

Also, (C) can be improved by noting that if $N \mid 2^n - 1$, n odd, then $[2^{(n+1)/2}]^2 \equiv 2 \pmod N$. But if 2 is a quadratic residue of N, then every factor of N will be congruent to $\pm 1 \pmod 8$. If further, $N \equiv -1 \pmod 8$, then there is at least one

factorization $N = ab$, where $a = tn + 1 \equiv 1 \pmod 8$ and $b = un + 1 \equiv -1 \pmod 8$. Thus, $8 \mid t$ and $2 \mid u$, and (C) becomes $x \equiv \frac{1}{2}(N + 1) \pmod{8n^2}$. If, on the other hand, $N \equiv 1 \pmod 8$, the best that can be obtained is that $2 \mid t$ and $2 \mid u$, whence $x \equiv \frac{1}{2}(N + 1) \pmod{2n^2}$.

We observe in (D) that the modulus can be increased by a factor of 2 if $(N - 1)/n$ is odd. (This condition often holds, as in the factorizations (2), (7), (15), and (39).) If we rewrite (B) as $(N - 1)/n = tun + t + u$, then since n is even, $t + u$ is odd. Hence, tu is even, say $2m$, and (C) becomes $N = 2mn^2 + 2x - 1$. Thus, $x \equiv \frac{1}{2}(N + 1) \pmod{n^2}$.

3. Primality Testing. (a) The main theorem we have used for primality testing is due to Lehmer [11]:

THEOREM 1. *If there exists an a such that $a^{N-1} \equiv 1 \pmod N$, but $a^{(N-1)/q} \not\equiv 1 \pmod N$ for every prime divisor q of $N - 1$, then N is prime.*

Since this theorem requires a knowledge of the complete factorization of $N - 1$, as well as a successful choice of the base a for which all the hypotheses hold, a certain amount of auxiliary calculation is necessary before the primality test can be completed (see Robinson [17]).

Accompanying the factorizations below, in which Theorem 1 was used, are the complete factorization of $N - 1$ and a primitive root a of N, to assist anyone who wishes to repeat our testing.

It is clear in some cases that the factorization of $N - 1$ is materially assisted by the form of N (see Lehmer [11]) as in (12), where $N = (2^{104} + 1)/257$ and $N - 1 = 2^8(2^{96} - 1)/257$, which readily factors.

In many of the calculations, such as (17), the theorem had to be applied several times to the cofactors at various "levels" before a final decision could be made concerning the primality of the original cofactor (see Brillhart [1]). In such cases the base used at each level is given in addition to the relevant factorization of one less than the cofactor under consideration.

It will be noted that the size of the bases used in testing (31) implies it was difficult to find a small primitive root for which the hypotheses of the theorem were all satisfied. It is of interest, then, to observe that the condition that the hypotheses hold for the *same* base can be relaxed to allow a change of base, if needed, for each prime factor of $N - 1$. In fact, we now have the following theorem of the second author:

THEOREM 2. *Let N be an odd integer >1. If $N - 1 = \prod p_i^{\alpha_i}$, q_i prime, and if for each q_i there exists an a_i for which $a_i^{N-1} \equiv 1 \pmod N$, but $a_i^{(N-1)/q_i} \not\equiv 1 \pmod N$, then N is prime.*

Proof. Let a_i belong to the exponent $d_i \pmod N$. Then $d_i \mid \phi(N)$. Let $D = LCM(d_i)$. Then $D \mid \phi(N)$. But $d_i \mid N - 1$, and $d_i \nmid (N - 1)/q_i$. Hence, $q_i^{\alpha_i} \mid d_i$ and thus $q_i^{\alpha_i} \mid D$. Then $N - 1 \mid D$, and finally $N - 1 \mid \phi(N)$, which implies that N is prime.

It is clear in practice that Theorem 2 is an improvement on Theorem 1, since if an a can be found for which $a^{N-1} \equiv 1 \pmod N$, but $a^{(N-1)/q} \not\equiv 1 \pmod N$ for a particular q, then that q has been settled once and for all, regardless of what bases are used for the other q's.

To illustrate Theorem 2 we note that the primality of the cofactor in (12)

can be decided with $a = 3$ for $q = 3, 5, 13, 17, 97, 193, 241, 673, 65537$, and 22253377; with $a = 7$ for $q = 7$; and with $a = 11$ for $q = 2$. However, in the list below we have taken the trouble to find a primitive root, rather than apply Theorem 2.

It should be pointed out that there is another theorem of Lehmer (p. 331 of [11]), which is generally superior to Theorem 2 in that it allows a change of base and requires that $N - 1$ be factored only up to the point where its factored part exceeds its unfactored part. Since no advantage was gained from this theorem in the present investigation, where either the full factorization of $N - 1$ was known, or not enough was known to apply this theorem, we have not used it here (see Theorem 3, p. 704 in Robinson [17]).

(b) Recently another test for primality has been programmed for the IBM 7090 by D. H. Lehmer. This test is based on a theorem concerning the divisibility properties of the Lucas sequences $U_{n+1} = PU_n - QU_{n-1}$, $n \geqq 1$, $U_0 = 0$, $U_1 = 1$, P and Q integers (see Lehmer [12, p. 442]): If $U_{N+1} \equiv 0 \pmod{N}$ and if $U_{m_i} \not\equiv 0 \pmod{N}$, where $m_i = (N + 1)/q_i$ for each prime factor q_i in $N + 1$, then N is a prime.

In the testing program, P is taken to be 1 and Q is chosen so that $(D/N) = -1$ and $(QD, N) = 1$, where $D = 1 - 4Q$. A discussion of this test will appear elsewhere in a paper of Professor Lehmer (for a special case see p. 18 of Lehmer [13]). We have used this program to show the completeness of (32) and the factorization of $2^{109} - 1$ in Section 4.

The advantage of this test, of course, is that it employs the factorization of $N + 1$, rather than $N - 1$, so that in case the complete factorization of $N - 1$ is not obtainable (or even the factorization to the square root of $N - 1$), we may still be able to factor $N + 1$. In those cases mentioned above where the factorization of $N + 1$ was used, we have given the value of Q at each level.

4. Miscellaneous Results. We begin this collection of results by pointing out that the factorizations (1)–(4), (7), (11), (14), (15), (17), (20), and (29) supplement the earlier paper of Brillhart [2] and complete the table there through $p < 100$. In this listing we have made no attempt to credit the previously known factors to their original discoverers; however, we would like to mention that the 7-digit factors in (34) and (39) are due to R. M. Merson, and were transmitted to us by K. R. Isemonger. Many of the factors, of course, can be found in Cunningham [3].

We have verified the following two complete factorizations due respectively to D. H. Lehmer (1957, unpublished):

$$2^{93} - 2^{47} + 1 = 5 \cdot 8681 \cdot 49477 \cdot \mathbf{4611545283086450689},$$

$$N - 1 = 2^{16} \cdot 3 \cdot 7 \cdot 31 \cdot 151 \cdot 715827883, \qquad a = 11;$$

and E. Gabard [4]:

$$2^{109} - 1 = \mathbf{745988807} \cdot \mathbf{870035986098720987332873},$$

$$N + 1 = 2 \cdot 3 \cdot 67 \cdot 83 \cdot 233 \cdot 111912126900880183, \qquad Q = 5,$$

$$N_1 - 1 = 2 \cdot 3 \cdot 503 \cdot 1801 \cdot 7643 \cdot 2693893, \qquad a = 3.$$

TABLE 1

p	Character of $2^p - 1$
2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127	Prime
(All other p under 135), 151, 163, 179, 181	Composite. Completely factored
167, 197, 233, 239, 241	Cofactor is a pseudoprime
157, 173, 191, 193, 211, 223, 229, 251	Cofactor is composite
137, 139, 149, 199, 227, 257	Composite but no factor known

In Brillhart [1] the numbers $N_p = (10^p - 1)/9$, p prime, are shown to be prime for $p = 2$, 19, and 23, and for no other $p \leqq 109$. We have extended the search for primes of this form, but there are no further primes for $p < 359$. This result was obtained by showing that $a^{N_p - 1} \not\equiv 1 \pmod{N_p}$ for those N_p for which no factor was known. For each N_p this test was run twice for $a = 3$ with complete agreement in the final remainders.

We have also examined the classical Mersenne numbers $M_p = 2^p - 1$, p prime $\leqq 257$, whose cofactors were of unknown character. The results of this investigation are given in Table 1 below. This table should be self-explanatory, except perhaps for the term "pseudoprime", which is used in the literature in several different ways.

In our usage, the term refers to an integer $N > 2$ which satisfies the congruence $a^{N-1} \equiv 1 \pmod{N}$ for some base a, $1 < a < N - 1$. This definition is in contrast to several others in which a "pseudoprime" is taken to be some composite solution of this congruence (see Shanks [19]).

We have found in practice that a number N with no particular form will generally turn out to be a prime if it is a pseudoprime for even a single base. This is due, no doubt, to the relative scarcity of composite pseudoprimes. A further indication of this scarcity is found in the fact that we have never encountered a composite pseudoprime in testing hundreds of numbers, even though infinitely many of them are known to exist (see Lehmer [14], Robinson [17]).

On the other hand, there are infinitely many numbers N with a special form, which we know are pseudoprimes for a particular base, but which we still cannot conclude are likely to be prime for this reason. A pertinent example of this is: $a = 2$ and N a primitive factor of $2^n - 1$, in which case we know that $N = kn + 1$, and hence that $2^{N-1} = 2^{kn} \equiv 1 \pmod{N}$. Thus, the term "pseudoprime" as used in Table 1 should be understood to refer to the base 3.

We conclude these results with a list of all the cases of complete factorizations of $2^n \pm 1$ that we have seen (Table 2). This brings up to date similar lists in Lehmer [15] and Robinson [18]. The more recent factorizations will be found in Math. Comp. (MTAC) with the exception of the following (listed with the name of their discoverer):

$$2^{78} - 2^{39} + 1 = 3 \cdot 19 \cdot \mathbf{530230622637030768 1801} \quad \text{(Gabard)}$$

$$2^{81} - 2^{41} + 1 = 13 \cdot 37 \cdot 279073 \cdot \mathbf{3618757} \cdot \mathbf{4977454861} \quad \text{(Merson)}$$

$$2^{86} + 2^{43} + 1 = 7 \cdot \mathbf{1105303606504929475345 9639} \quad \text{(Gabard)}$$

$$2^{101} - 1 = \mathbf{7432339208719} \cdot \mathbf{341117531003194129} \quad \text{(G. D. Johnson)}$$

$$2^{101} + 1 = 3 \cdot \mathbf{845100400152152934331135470251} \quad \text{(Gabard)}$$

$$2^{115} - 2^{58} + 1 = 5^2 \cdot \mathbf{461} \cdot 1013 \cdot 1657 \cdot \mathbf{5981} \cdot \mathbf{359006912765190408181} \quad \text{(Isemonger)}$$

$$2^{115} + 1 = 3 \cdot 11 \cdot \mathbf{691} \cdot 2796203 \cdot \mathbf{1884103651} \cdot \mathbf{345767385170491} \quad \text{(Isemonger)}$$

$$2^{119} - 2^{60} + 1 = 113 \cdot 137 \cdot 953 \cdot \mathbf{2381} \cdot \mathbf{42841} \cdot \mathbf{823481} \cdot \mathbf{536296539263941} \quad \text{(Isemonger)}$$

$$2^{122} + 2^{61} + 1 = \mathbf{7} \cdot \mathbf{367} \cdot \mathbf{55633} \cdot \mathbf{372017086253051463039733520 41} \quad \text{(Gabard)}$$

$$2^{125} + 2^{63} + 1 = 41 \cdot 101 \cdot \mathbf{7001} \cdot 8101 \cdot \mathbf{3775501} \cdot \mathbf{47970133603445383501} \quad \text{(Isemonger)}$$

$$2^{143} + 2^{72} + 1 = 5 \cdot 397 \cdot 1613 \cdot \mathbf{25741} \cdot \mathbf{3426853} \cdot \mathbf{9467173} \cdot \mathbf{4170165570896115649} \quad \text{(Isemonger)}$$

$$2^{147} - 2^{74} + 1 = 5 \cdot 29 \cdot 197 \cdot 14449 \cdot \mathbf{540961} \cdot 19707683773 \cdot \mathbf{405448596935211523 69} \quad \text{(Isemonger)}$$

$$2^{153} - 2^{77} + 1 = 13 \cdot 37 \cdot 137 \cdot 953 \cdot \mathbf{2582029} \cdot \mathbf{4260133} \cdot 1326700741 \cdot \mathbf{12458723489217613} \quad \text{(Merson)}$$

TABLE 2

$2^n - 1$, n odd: n = 1–123, 127–135, 147, 151–155, 159, 163, 165, 171, 175, 179, 181, 189, 195, 201, 225, 255, 315, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213.

$2^n + 1$: n = 0–102, 104–118, 120, 122, 123, 126, 129, 130, 132, 134, 135, 138, 141, 142, 144, 146–148, 150, 154, 158, 162, 165, 166, 170, 174, 178, 182, 186, 190, 194, 195, 198, 201, 206, 210, 214, 222, 226, 230, 234, 246, 250, 270.

$2^n - 2^m + 1$, $n = 2m - 1$: n = 1–99, 103–107, 111–119, 123–127, 135, 141, 147, 151, 153, 165, 167, 239, 241, 353, 367, 457.

$2^n + 2^m + 1$, $n = 2m - 1$: n = 1–99, 103–117, 123, 125, 129, 135, 143, 157, 163, 171, 283, 379.

5. Acknowledgments. We would like to express our gratitude to K. R. Isemonger for his assistance in the present work. We would also like to state our indebtedness to the Department of Mathematics at UCLA for sponsoring this investigation. Finally, we wish to thank D. H. Lehmer for his continuing interest and active contributions to the results of this paper.

Complete Factorizations

1. $2^{79} + 2^{40} + 1 = 5 \cdot \mathbf{317} \cdot \mathbf{381364611866507317969}$
   $N - 1 = 2^4 \cdot 3^2 \cdot 79 \cdot 36558773 \cdot 916978591, \quad a = 11,$

2. $2^{83} + 2^{42} + 1 = \mathbf{997 \cdot 46202197673 \cdot 209957719973}$

3. $2^{89} - 2^{45} + 1 = \mathbf{1069 \cdot 579017791994999956106149}$
   $N - 1 = 2^2 \cdot 3^7 \cdot 89 \cdot 109 \cdot 6199 \cdot 1100639243449, \quad a = 6,$

4. $2^{89} + 2^{45} + 1 = 5 \cdot \mathbf{1237940039285450643643301 89}$
   $N - 1 = 2^2 \cdot 3^2 \cdot 23 \cdot 89 \cdot 397 \cdot 683 \cdot 2113 \cdot 2932031007403, \quad a = 6,$

5. $2^{95} - 2^{48} + 1 = 41 \cdot \mathbf{761} \cdot 525313 \cdot \mathbf{2416923620660807201}$
   $N - 1 = 2^5 \cdot 5^2 \cdot 19 \cdot 159008132938211, \quad a = 13,$
   $N_1 - 1 = 2 \cdot 5 \cdot 23 \cdot 31 \cdot 6829 \cdot 3265673, \quad a_1 = 17,$

6. $2^{96} - 2^{48} + 1 = \mathbf{1153 \cdot 6337 \cdot 38941695937 \cdot 278452876033}$

7. $2^{97} - 2^{49} + 1 = \mathbf{389 \cdot 4657 \cdot 4959325597 \cdot 17637260034881}$

8. $2^{98} - 2^{49} + 1 = 3 \cdot 5419 \cdot \mathbf{748819 \cdot 26032885845392093851}$
   $N - 1 = 2 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 13 \cdot 617 \cdot 147192338057, a = 7,$

9. $2^{98} + 2^{49} + 1 = 7^3 \cdot 337 \cdot \mathbf{27416723625287255350687 27}$
   $N - 1 = 2 \cdot 3 \cdot 7^2 \cdot 61 \cdot 337 \cdot 70687 \cdot 6417545220131, \quad a = 3,$

10. $2^{102} + 2^{51} + 1 = 73 \cdot \mathbf{919 \cdot 755824884241793470834383 19}$
    $N - 1 = 2 \cdot 3^2 \cdot 17 \cdot 67 \cdot 853 \cdot 5399 \cdot 800502326409847, \quad a = 6,$
    $N_1 - 1 = 2 \cdot 3 \cdot 41 \cdot 43 \cdot 75676151107, \quad a_1 = 5,$

11. $2^{103} + 2^{52} + 1 = 5 \cdot \mathbf{17325013 \cdot 117070097457656623005977}$
    $N - 1 = 2^3 \cdot 59 \cdot 103 \cdot 162917 \cdot 14780882080883, \quad a = 19,$

12. $2^{104} + 1 = 257 \cdot \mathbf{78919881726271091143763623681}$
    $N - 1 = 2^8 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 97 \cdot 193 \cdot 241 \cdot 673 \cdot 65537 \cdot 22253377, \quad a = 61,$

13. $2^{107} + 1 = 3 \cdot \mathbf{643 \cdot 84115747449047881488635567801}$
    $N - 1 = 2^3 \cdot 5^2 \cdot 107 \cdot 39306424041611159574128 77, \quad a = 41,$
    $N_1 - 1 = 2^2 \cdot 3^2 \cdot 71 \cdot 747619 \cdot 1020797 \cdot 2015036747, \quad a_1 = 5,$

14. $2^{107} - 2^{54} + 1 = 5 \cdot \mathbf{857 \cdot 37866809061660057264219253397}$
    $N - 1 = 2^2 \cdot 19 \cdot 107 \cdot 353 \cdot 91813 \cdot 143675413657196977, \quad a = 21,$
    $N_1 - 1 = 2^4 \cdot 3^2 \cdot 547 \cdot 1103 \cdot 1653701519, \quad a_1 = 5,$

15. $2^{107} + 2^{54} + 1 = \mathbf{843589 \cdot 8174912477117 \cdot 23528569104401}$

16. $2^{109} + 1 = 3 \cdot \mathbf{104124649 \cdot 20777568473623488631 28179}$
    $N - 1 = 2 \cdot 3 \cdot 29 \cdot 109 \cdot 21427369 \cdot 5112697847507, \quad a = 3,$

17. $2^{109} + 2^{55} + 1 = \mathbf{5669 \cdot 666184021 \cdot 171857646012809566969}$
    $N - 1 = 2^3 \cdot 3 \cdot 19 \cdot 109 \cdot 3457622042749267, \quad a = 7,$
    $N_1 - 1 = 2 \cdot 3 \cdot 7 \cdot 82324334351173, \quad a_1 = 5,$
    $N_2 - 1 = 2^2 \cdot 3 \cdot 210559 \cdot 32575469, \quad a_2 = 5,$

18. $2^{110} + 2^{55} + 1 = 7 \cdot 151 \cdot 599479 \cdot \mathbf{204856883529738048676 0231}$
    $N - 1 = 2 \cdot 3 \cdot 5 \cdot 11 \cdot 31 \cdot 29527 \cdot 6781965931002463, \quad a = 6,$
    $N_1 - 1 = 2 \cdot 3 \cdot 41 \cdot 491 \cdot 811 \cdot 69233797, \quad a_1 = 6,$

19. $2^{111} - 2^{56} + 1 = 13 \cdot 593 \cdot 231769777 \cdot \mathbf{1453030298001690873541}$
    $N - 1 = 2^2 \cdot 3 \cdot 5 \cdot 37 \cdot 109 \cdot 302663 \cdot 19839734921, \quad a = 7,$

20. $2^{113}+2^{57}+1 = 5\cdot\mathbf{58309}\cdot\mathbf{2362153}\cdot\mathbf{150791162139013261783 69}$
$N-1 = 2^6\cdot 3^2\cdot 7^2\cdot 89\cdot 113\cdot 1373\cdot 191281\cdot 202277, \quad a = 11,$

21. $2^{114}+2^{57}+1 = 73\cdot\mathbf{93507247}\cdot\mathbf{304264563479254131203 7847}$
$N-1 = 2\cdot 3^2\cdot 7\cdot 19\cdot 23^2\cdot 7823\cdot 307113018359177, \quad a = 6,$
$N_1-1 = 2^3\cdot 156841\cdot 244764617, \quad a_1 = 3,$

22. $2^{116}+1 = 17\cdot\mathbf{59393}\cdot\mathbf{82280195167144119832390568177}$
$N-1 = 2^4\cdot 13\cdot 17\cdot 29\cdot 71\cdot 89\cdot 580231\cdot 218844570055711, \quad a = 3,$
$N_1-1 = 2\cdot 3\cdot 5\cdot 19\cdot 23\cdot 39371\cdot 423991, \quad a_1 = 19,$

23. $2^{117}-2^{59}+1 = 5\cdot 109\cdot 1613\cdot 3121\cdot\mathbf{7489}\cdot 21841\cdot\mathbf{370244405487013669}$
$N-1 = 2^2\cdot 3^4\cdot 13\cdot 1360283\cdot 64620583, \quad a = 17,$

24. $2^{121}-1 = 23\cdot 89\cdot\mathbf{727}\cdot\mathbf{178639387836316422785 8270210279}$
$N-1 = 2\cdot 3^3\cdot 11^2\cdot 27339973651104441809890 8817, \quad a = 6,$
$N_1-1 = 2^4\cdot 3^2\cdot 47\cdot 79\cdot 103\cdot 211\cdot 75983\cdot 309652459427, \quad a_1 = 10,$

25. $2^{123}-2^{62}+1 = 5\cdot 10169\cdot 43249589\cdot\mathbf{802333429}\cdot\mathbf{6027043735173469}$
$N-1 = 2^2\cdot 3\cdot 7\cdot 41\cdot 587\cdot 27241\cdot 109441, \quad a = 11,$

26. $2^{123}+2^{62}+1 = 13\cdot\mathbf{2953}\cdot 181549\cdot 12112549\cdot\mathbf{1259659769763925643 17}$
$N-1 = 2^2\cdot 3\cdot 41\cdot 127\cdot 467\cdot 9803\cdot 440360699, \quad a = 7,$

27. $2^{125}-2^{63}+1 = 5^4\cdot\mathbf{28001}\cdot\mathbf{96001}\cdot 268501\cdot\mathbf{94291866932171243501}$
$N-1 = 2^2\cdot 5^3\cdot 11\cdot 557\cdot 1603673\cdot 19192897, \quad a = 29,$

28. $2^{126}+2^{63}+1 = 262657\cdot\mathbf{1560007}\cdot\mathbf{207617485544258392970753527}$
$N-1 = 2\cdot 3^3\cdot 7\cdot 43\cdot 109\cdot 3449\cdot 376889\cdot 90150993481, \quad a = 5,$

29. $2^{127}-2^{64}+1 = \mathbf{509}\cdot\mathbf{26417}\cdot\mathbf{140385293}\cdot\mathbf{901335669179135177 09497}$
$N-1 = 2^3\cdot 3\cdot 127\cdot 29571380222412571427, \quad a = 7,$
$N_1-1 = 2\cdot 13\cdot 1061802263\cdot 1071160627, \quad a_1 = 6,$

30. $2^{130}-2^{65}+1 = 3.331\cdot\mathbf{107251}\cdot 22366891\cdot\mathbf{57140392112607695718 2161}$
$N-1 = 2^4\cdot 3\cdot 5\cdot 13\cdot 183142282412204152943, \quad a = 19,$
$N_1-1 = 2\cdot 23\cdot 3981353965482698977, \quad a_1 = 5,$
$N_2-1 = 2^5\cdot 3\cdot 71\cdot 941\cdot 52571\cdot 11807701, \quad a_2 = 5,$

31. $2^{130}+2^{65}+1 = 7\cdot 79\cdot 151\cdot 121369\cdot\mathbf{13430419684509926257281457335 1}$
$N-1 = 2\cdot 3^2\cdot 5^2\cdot 7\cdot 11\cdot 13\cdot 298155615151735514647163, \quad a = 29,$
$N_1-1 = 2\cdot 13\cdot 19\cdot 86573\cdot 6971617904258551, \quad a_1 = 37,$
$N_2-1 = 2\cdot 3\cdot 5^2\cdot 83\cdot 559969309579, \quad a_2 = 37,$

32. $2^{131}-1 = \mathbf{263}\cdot\mathbf{10350794431055162386718619237468234569}$
$N+1 = 2\cdot 3\cdot 5\cdot 7^2\cdot 11^2\cdot 2711\cdot 21465522331181621122125609701, \quad Q = 17,$
$N_1+1 = 2\cdot 3^3\cdot 89^2\cdot 30211\cdot 1661126041959455923, \quad Q_1 = 29,$
$N_2+1 = 2^2\cdot 389\cdot 22901\cdot 46616380229, \quad Q_2 = 1,$

33. $2^{133}-1 = 127\cdot 524287\cdot\mathbf{16353722085272539885143432572 0959}$
$N-1 = 2\cdot 3^4\cdot 7\cdot 19\cdot 23\cdot 73\cdot 252313\cdot 77555939\cdot 231017337191, \quad a = 3,$

34. $2^{134} - 2^{67} + 1 = 3 \cdot \mathbf{2011} \cdot \mathbf{9649} \cdot \mathbf{6324667} \cdot \mathbf{59151549118532676874448563}$
$N - 1 = 2 \cdot 3^3 \cdot 7^2 \cdot 13 \cdot 67 \cdot 1381 \cdot 2861 \cdot 6496008606077, \quad a = 3,$

35. $2^{134} + 2^{67} + 1 = 7 \cdot \mathbf{1609} \cdot \mathbf{22111} \cdot \mathbf{87449423397425857942678833145441}$
$N - 1 = 2^5 \cdot 3 \cdot 5 \cdot 13 \cdot 67 \cdot 1559 \cdot 4027 \cdot 15053 \cdot 1681973 \cdot 1315914679, \quad a = 29,$

36. $2^{150} + 2^{75} + 1 = 73 \cdot 631 \cdot 23311 \cdot \mathbf{115201} \cdot \mathbf{617401} \cdot \mathbf{1348206751}$
$\cdot \mathbf{13861369826299351}$
$N - 1 = 2 \cdot 3^2 \cdot 5^2 \cdot 41 \cdot 1933 \cdot 388667231, \quad a = 3,$

37. $2^{155} - 1 = 31^2 \cdot 311 \cdot \mathbf{11471} \cdot \mathbf{73471} \cdot 2147483647 \cdot \mathbf{4649919401} \cdot \mathbf{18158209813151}$

38. $2^{170} + 2^{85} + 1 = 7 \cdot 103 \cdot 151 \cdot 2143 \cdot 11119 \cdot \mathbf{106591} \cdot \mathbf{949111}$
$\cdot \mathbf{57024515776397755458386431 51}$
$N - 1 = 2 \cdot 3 \cdot 5^2 \cdot 11 \cdot 17 \cdot 1163 \cdot 1471 \cdot 5197 \cdot 43793 \cdot 522130351, \quad a = 13,$

39. $2^{171} + 2^{86} + 1 = 13 \cdot 37 \cdot \mathbf{25309} \cdot 131101 \cdot 160969 \cdot 525313 \cdot \mathbf{5675149}$
$\cdot \mathbf{39291697} \cdot \mathbf{99463730244517}$

40. $2^{175} - 1 = 31 \cdot 71 \cdot 127 \cdot 601 \cdot 1801 \cdot \mathbf{39551} \cdot 122921 \cdot \mathbf{60816001}$
$\cdot \mathbf{53534762479148855283715 1}$
$N - 1 = 2 \cdot 5^2 \cdot 7 \cdot 97 \cdot 137 \cdot 331 \cdot 261389 \cdot 1330332599, \quad a = 13,$

41. $2^{210} + 2^{105} + 1 = 73 \cdot 631 \cdot 23311 \cdot 92737 \cdot 649657 \cdot \mathbf{870031} \cdot \mathbf{983431}$
$\cdot \mathbf{29728307155963706810228435378401}$
$N - 1 = 2^5 \cdot 3^2 \cdot 5^2 \cdot 7 \cdot 19 \cdot 3361 \cdot 11329 \cdot 3163739 \cdot 257706459649, \quad a = 23.$

Department of Mathematics
University of California
Berkeley, California

Department of Mathematics
Penn State University
State College, Pennsylvania

1. J. BRILLHART, "Some miscellaneous factorizations," *Math. Comp.*, v. 17, 1963, pp. 447–450.
2. J. BRILLHART, "Concerning the numbers $2^{2^p} + 1$, p prime," *Math. Comp.*, v. 16, 1962, pp. 424–430. MR **26** #6100.
3. A. J. C. CUNNINGHAM & H. J. WOODALL, *Factorizations of* $(y^n \mp 1)$, Hodgson, London, 1925.
4. E. GABARD, "Factorisation d'un nouveau nombre de Mersenne," *Mathesis*, 1959, p. 61.
5. D. JARDEN, *Recurring Sequences*, Riveon Lematematika, v. 12, 1958, pp. 18–39. (Hebrew)
6. M. KRAITCHIK, *Recherches sur la Théorie des Nombres*, Tome II, Paris, 1929.
7. D. H. LEHMER, "The mechanical combination of linear forms," *Amer. Math. Monthly*, v. 35, 1928, pp. 114–121.
8. D. H. LEHMER, "A photo electric number sieve," *Amer. Math. Monthly*, v. 40, 1933, pp. 401–406.
9. D. H. LEHMER, "A machine for combining sets of linear congruences," *Math. Ann.*, v. 109, 1934, pp. 661–667.
10. D. H. LEHMER, "On the factorization of Lucas' functions," *Tôhoku Math. J.*, v. 34, 1931, pp. 1–7.
11. D. H. LEHMER, "Tests for primality by the converse of Fermat's theorem," *Bull. Amer. Math. Soc.*, v. 33, 1927, pp. 327–340.
12. D. H. LEHMER, "An extended theory of Lucas' functions," *Ann. of Math.*, v. 31, 1930, pp. 419–448.
13. D. H. LEHMER, "The primality of Ramanujan's Tau-function," *Amer. Math. Monthly*, Slaught Mem. Papers, *Computers and Computing*, no. 10, 1965, pp. 15–18.

→ D. H. LEHMER, "On the converse of Fermat's theorem," *Amer. Math. Monthly*, v. 43, 1936, pp. 347–354.

15. D. H. LEHMER, *Guide to Tables in the Theory of Numbers*, Bulletin of the National Research Council, v. 105, Washington, D. C., 1941, pp. 29–30. MR **2**, 247.

16. D. N. LEHMER, "Hunting big game in the theory of numbers," *Scripta Math.*, 1933, pp. 229–235.

→ R. M. ROBINSON, "The converse of Fermat's theorem," *Amer. Math. Monthly*, v. 64, 1957, pp. 703–710. MR **20** #4520.

18. R. M. ROBINSON, "Some factorizations of numbers of the form $2^n \pm 1$," *MTAC*, v. 11, 1957, pp. 265–268. MR **20** #832.

19. D. SHANKS, *Solved and Unsolved Problems in Number Theory*, Vol. I, Spartan, Washington, D. C., 1962, pp. 115–120. MR **28** #3952.

20. J. V. USPENSKY & M. A. HEASLET, *Elementary Number Theory*, McGraw-Hill, New York, 1939, pp. 317–323. MR **1**, 38.