A REPORT ON PRIMES OF THE FORM $k \cdot 2^n + 1$ AND ON FACTORS OF FERMAT NUMBERS

RAPHAEL M. ROBINSON

This note is a report on some calculations carried out during 1956 and 1957 on the SWAC, a high-speed computer located on the Los Angeles campus of the University of California, and supported in part by the Office of Naval Research. A preliminary report appeared in [11], and a few copies of a large table [12] were printed. The routines used on the SWAC were prepared by the author. My thanks are due to John L. Selfridge for assistance in operating the computer, and for valuable suggestions.

1. **Primes of the form $k \cdot 2^n + 1$.** Since every number $N > 1$ can be put in the form $N = k \cdot 2^n + 1$, with k odd, $k > 0$, and $n \geqq 0$, the only meaning which can be attached to describing a number as being of this form is a rather vague one, namely that the value of k involved is relatively small. In the course of our computation, all of these numbers with $k < 100$ and $n < 512$ were tested for primeness, as well as some numbers lying outside of this range.

A preliminary sieve routine was used to look for small factors of N. Actually, the smallest factor was found if less than 10^5 when $k \leqq 7$, and if less than 10^4 otherwise. If no small factor was found, the number N was tested for primeness using a theorem stated by Proth in 1878: *Let* $N = k \cdot 2^n + 1$, *where* $0 < k < 2^n$. *Suppose that* $(a/N) = -1$. *Then* N *is prime if and only if* $a^{(N-1)/2} \equiv -1 \pmod{N}$. For a discussion of this and related results, see [14], where this test appears as Theorem 9. The first step in applying the test was to find a suitable value of a; if k is not a multiple of 3, we may take $a = 3$, and in any case finding a does not present any difficulty. The time for the test did not exceed a minute and a half as long as $n < 512$. For $k = 3, 5, 7$, some larger values of n were also used; the time for the test was about seven minutes for n near 1000. The only cases to which the test does not apply are those where n is very small, and here no test is needed. Also, when $k = 1$ the test was omitted, since the character of $2^n + 1$ was already known for $n < 8192$; see [10].

A list of the primes found for $k < 100$ appears in Table 1. The list is complete in all cases for $n < 512$, and for the first few cases in a larger range, namely:

Received by the editors April 7, 1958.

TABLE 1. LIST OF PRIMES OF THE FORM $k \cdot 2^n + 1$.

k	n
1	0, 1, 2, 4, 8, 16
3	1, 2, 5, 6, 8, 12, 18, 30, 36, 41, 66, 189, 201, 209, 276, 353, 408, 438, 534
5	1, 3, 7, 13, 15, 25, 39, 55, 75, 85, 127, 1947
7	2, 4, 6, 14, 20, 26, 50, 52, 92, 120, 174, 180, 190, 290, 320, 390, 432, 616, 830
9	1, 2, 3, 6, 7, 11, 14, 17, 33, 42, 43, 63, 65, 67, 81, 134, 162, 206, 211, 366
11	1, 3, 5, 7, 19, 21, 43, 81, 125, 127, 209, 211
13	2, 8, 10, 20, 28, 82, 188, 308, 316
15	1, 2, 4, 9, 10, 12, 27, 37, 38, 44, 48, 78, 112, 168, 229, 297, 339
17	3, 15, 27, 51, 147, 243, 267, 347, 471
19	6, 10, 46, 366
21	1, 4, 5, 7, 9, 12, 16, 17, 41, 124, 128, 129, 187, 209, 276, 313, 397
23	1, 9, 13, 29, 41, 49, 69, 73, 341, 381, 389
25	2, 4, 6, 10, 20, 22, 52, 64, 78, 184, 232, 268, 340, 448
27	2, 4, 7, 16, 19, 20, 22, 26, 40, 44, 46, 47, 50, 56, 59, 64, 92, 175, 215, 275, 407, 455
29	1, 3, 5, 11, 27, 43, 57, 75, 77, 93, 103, 143, 185, 231, 245, 391
31	8, 60, 68, 140, 216, 416
33	1, 6, 13, 18, 21, 22, 25, 28, 66, 93, 118, 289, 412, 453
35	1, 3, 7, 9, 13, 15, 31, 45, 47, 49, 55, 147, 245, 327, 355
37	2, 4, 8, 10, 12, 16, 22, 26, 68, 82, 84, 106, 110, 166, 236, 254, 286, 290
39	1, 2, 3, 5, 7, 10, 11, 13, 14, 18, 21, 22, 31, 42, 67, 70, 71, 73, 251, 370, 375, 389, 407
41	1, 11, 19, 215, 289, 379
43	2, 6, 12, 18, 26, 32, 94, 98, 104, 144, 158, 252
45	2, 9, 12, 14, 23, 24, 29, 60, 189, 200, 333, 372, 443, 464
47	
49	2, 6, 10, 30, 42, 54, 66, 118, 390

TABLE 1. LIST OF PRIMES OF THE FORM $k \cdot 2^n + 1$.

k	n
51	1, 3, 7, 9, 13, 17, 25, 43, 53, 83, 89, 92, 119, 175, 187, 257, 263, 267, 321, 333
53	1, 5, 17, 21, 61, 85, 93, 105, 133, 485
55	4, 8, 16, 22, 32, 94, 220, 244, 262, 286, 344, 356, 392
57	2, 3, 7, 8, 10, 16, 18, 19, 40, 48, 55, 90, 96, 98, 190, 398, 456, 502
59	5, 11, 27, 35, 291
61	4, 12, 48, 88, 168
63	1, 4, 5, 9, 10, 14, 17, 18, 21, 25, 37, 38, 44, 60, 65, 94, 133, 153, 228, 280, 314, 326, 334, 340, 410, 429
65	1, 3, 5, 11, 17, 21, 29, 47, 85, 93, 129, 151, 205, 239, 257, 271, 307, 351, 397, 479
67	2, 6, 14, 20, 44, 66, 74, 102, 134, 214, 236, 238, 342, 354, 382, 454, 470
69	1, 2, 10, 14, 19, 26, 50, 55, 145
71	3, 5, 9, 19, 23, 27, 57, 59, 65, 119, 299, 417
73	2, 6, 14, 24, 30, 32, 42, 44, 60, 110, 212, 230
75	1, 3, 4, 6, 7, 10, 12, 34, 43, 51, 57, 60, 63, 67, 87, 102, 163, 222, 247, 312, 397, 430
77	3, 7, 19, 23, 95, 287, 483
79	2, 10, 46, 206
81	1, 4, 5, 7, 12, 15, 16, 21, 25, 27, 32, 35, 36, 39, 48, 89, 104, 121, 125, 148, 152, 267, 271, 277, 296, 324, 344, 396, 421, 436, 447
83	1, 5, 157, 181, 233, 373
85	4, 6, 10, 30, 34, 36, 38, 74, 88, 94, 148, 200
87	2, 6, 8, 18, 26, 56, 78, 86, 104, 134, 207
89	1, 7, 9, 21, 37, 61
91	8, 168, 260
93	2, 4, 6, 10, 12, 30, 42, 44, 52, 70, 76, 108, 122, 164, 170, 226, 298, 398
95	1, 3, 5, 7, 13, 17, 21, 53, 57, 61, 83, 89, 111, 167, 175, 237
97	2, 4, 14, 20, 40, 266, 400
99	1, 2, 5, 6, 10, 11, 22, 31, 33, 34, 41, 42, 53, 58, 65, 82, 126, 143, 162, 170, 186, 189, 206, 211, 270, 319, 369, 410, 433

$$k = 1,\ n < 8192; \qquad k = 3,\ n < 1280; \qquad k = 5,\ n < 2005;$$
$$k = 7,\ n < 1280.$$

The calculations were checked by a second run, so that we can say with some assurance that Table 1 is accurate and complete to the stated bounds. Notice that there are no primes of the form $47 \cdot 2^n + 1$ with $n < 512$.

The checking of this table was finished in the spring of 1957, except that at this time the case $k = 5$ was complete only for $n < 1585$. In the fall of 1957, the range for $k = 5$ was extended to $n < 2005$. One additional prime was discovered, namely $5 \cdot 2^{1947} + 1$. Notice that there is not a single prime of the form $5 \cdot 2^n + 1$ with $127 < n < 1947$. The new prime is the largest in the table by far. It is the fourth largest prime known at present, the larger ones being the Mersenne primes $2^n - 1$ with $n = 3217$, 2281, and 2203; see Riesel [9] and Robinson [10].

In May 1957, eighteen copies of a table [12] of 312 pages were printed on a tabulator, giving the results of the computation. The table has been sent to a few libraries, and deposited in the Unpublished Mathematical Tables file of the journal *Mathematical Tables and Other Aids to Computation*. The smallest factor of $N = k \cdot 2^n + 1$ was printed where found. Otherwise, there was printed an indication whether N is prime or composite, and the value of the smallest positive a such that $(a/N) = -1$, which was used in testing N for primeness. The table is too bulky for publication, but the information of most interest, aside from the factors of Fermat numbers discussed in §2, is the character of N (prime or composite), and this can be determined from Table 1.

On the other hand, information of some interest, such as the fact that the smallest factor of $5 \cdot 2^{79} + 1$ is 98801, is necessarily lost in the condensation. Besides the smallest factors, another item eliminated is the smallest nonresidues. In this case, a summary appears to be of interest. The largest value of a which we encountered was $a = 47$. For $k < 100$, this appeared only for two composite values of N, namely $N = 33 \cdot 2^{172} + 1$ and $N = 69 \cdot 2^{365} + 1$. It did appear also for a prime $N = 1575 \cdot 2^{147} + 1$ which we had occasion to test. If we restrict ourselves to prime values of N with $k < 100$, we have the following empirical result.

THEOREM. *If $N = k \cdot 2^n + 1$ is prime, where k is odd, $0 < k < 100$, and $0 < n < 512$, then the smallest positive quadratic nonresidue of N does not exceed 23. The smallest nonresidue is 23 in just three cases*:

$$N = 39 \cdot 2^{13} + 1, \qquad 33 \cdot 2^{28} + 1, \qquad 57 \cdot 2^{90} + 1.$$

The numbers of the form $N=n\cdot 2^n+1$ are called Cullen numbers. They were studied by Cunningham and Woodall [2], who stated on page 22 that for just 47 of these numbers with $n\leqq 1000$ is the smallest factor greater than 1000. They give a factor in three of these cases. The remaining 44 numbers were tested on the SWAC, and of these only one turned out to be prime, namely $N=141\cdot 2^{141}+1$. Assuming the correctness of the results in [2], we can say that this is the only Cullen prime with $2\leqq n\leqq 1000$.

We now give a brief survey of earlier tables of primes of the form $k\cdot 2^n+1$ or of factors of numbers of this form. A short list of primes of the form $k\cdot 2^n+1$ was given by Seelhoff [15] in 1886. A comparison with Table 1 shows that there are several errors in his list. Cunningham [1, pp. 56–73], lists a number of primes of the form $k\cdot 2^n+1$, none exceeding 10^8, together with certain quadratic partitions. Kraitchik [5, pp. 12–13], gives the smallest factor of each number $N=k\cdot 2^n+1$ with k odd, $1<k<100$, and $2\cdot 10^8<N<10^{12}$. In Kraitchik [6, pp. 222–232], the range is extended to $0<k<1000$ and $10^8<N<10^{12}$, and a list of primes from the table appears on pp. 233–235. A comparison with the table [12] disclosed a number of errors on pp. 222–223. The following corrections may be noted.

k	n	FOR	READ	k	n	FOR	READ
13	23	5	3	57	32	442837	73
15	28	263	241	59	33	17	11
25	34	33461	2129	63	29	29	61
31	24	467	311	67	21	5	3
41	22	5	3	69	22	59	53
53	29	23	11	69	23	53	12227
57	21	3	5	71	25	977	13

In the eleven cases where Kraitchik's entry is too large, it turns out to be a factor also; in the other three cases, it cannot be. Finally, we mention a table of primes of the form $k\cdot 2^n-1$ given by Riesel [8].

2. **Factors of Fermat numbers.** If the number N turned out to be a prime, then it was also tested to find whether it is a factor of any Fermat number $F_m=2^{2^m}+1$. This carries out a project suggested in the last sentence of [10]. Since, for $m\geqq 2$, every prime factor p of F_m satisfies $p\equiv 1 \pmod{2^{m+2}}$, we needed to try the number $N=k\cdot 2^n+1$ as a factor of F_m only for $m\leqq n-2$. The routine for making this test was very similar to that used for testing N for primeness.

Besides testing the primes in Table 1 as factors of Fermat numbers, the numbers $k\cdot 2^n+1$ with $k=119$, 397, 579, 973, 1071, 1575, 11131,

and 52347, and with $n<256$, were also examined. These values of k were chosen because a prime factor of a Fermat number was already known in each case. One additional prime factor was found, corresponding to $k=1575$; in fact, $1575\cdot 2^{157}+1$ is a divisor of F_{150}. This factor, as well as thirteen with $k<100$, was given in the preliminary report [11]. The testing of the primes in Table 1 was completed in 1957, and two more factors of Fermat numbers were found, namely

$$95\cdot 2^{61}+1 \mid F_{58}, \qquad 5\cdot 2^{1947}+1 \mid F_{1945},$$

of which the first appears in [12]. Some further experimentation with values of $k>100$ was undertaken in 1957 by John L. Selfridge, using a modified form of my routine. Four other factors of Fermat numbers were found, namely

$$425\cdot 2^{79}+1 \mid F_{77}, \qquad 271\cdot 2^{84}+1 \mid F_{81},$$
$$403\cdot 2^{252}+1 \mid F_{250}, \qquad 177\cdot 2^{271}+1 \mid F_{267}.$$

A list of all known prime factors of composite Fermat numbers appears in Table 2, together with the date found or published, and the discoverer. See Dickson [3, Chapter XV], for references on Fermat numbers prior to 1918. Kraitchik's factor for $m=15$ is mentioned on page 220 of his book [6], and is misquoted on the following page. Selfridge's factors for $m=10$ and 16 were announced in [16]. In all, there are now 38 prime factors $k\cdot 2^n+1$ of 33 different composite Fermat numbers F_m known. As mentioned earlier, the difference $n-m$ is at least 2; the values of this difference which actually occur in the table are 2, 3, 4, 6, 7, 8.

It should also be recalled that F_m is prime for $m=0$, 1, 2, 3, 4. Furthermore, Morehead and Western showed some fifty years ago that F_7 and F_8 are composite, and their calculation was verified in [10], but no factor of either has been found. It was shown in [13] that there are no additional prime factors p of Fermat numbers with $p<2^{32}$, and also no additional factors $p<2^{35}$ such that $p\equiv 1 \pmod{2^{15}}$. In particular, F_7 is a product of either 2 or 3 prime factors, and F_{13} has no factor $p<2^{35}$. The character of F_{13} is still unknown.

The condition that a prime $N=k\cdot 2^n+1$ divides some Fermat number is exactly that 2 should be a kth power residue mod N. For 2 is a kth power residue mod N if and only if $2^{(N-1)/k}\equiv 1 \pmod{N}$, that is, $2^{2^n}\equiv 1 \pmod{N}$, and this is equivalent to having $2^{2^m}\equiv -1 \pmod{N}$, or $N \mid F_m$, for some $m<n$. This is not usually helpful in deciding whether N is a factor of any Fermat number, but there is one case in which it is, as is shown by the proof of the following theorem, which was given by Morehead [7].

TABLE 2. FACTORS $k \cdot 2^n + 1$ OF FERMAT NUMBERS F_m.

k	n	m	Date	Discoverer
5	7	5	1732	Euler
52347	7	5	1732	Euler
1071	8	6	1880	Landry
262814145745	8	6	1880	Landry, Le Lasseur
37	16	9	1903	Western
11131	12	10	1953	Selfridge (SWAC)
39	13	11	1899	Cunningham
119	13	11	1899	Cunningham
7	14	12	1877	Pervouchine, Lucas
397	16	12	1903	Western
973	16	12	1903	Western
579	21	15	1925	Kraitchik
1575	19	16	1953	Selfridge (SWAC)
13	20	18	1903	Western
5	25	23	1878	Pervouchine
5	39	36	1886	Seelhoff
3	41	38	1903	Cullen, Cunningham, Western
21	41	39	1956	Robinson (SWAC)
29	57	55	1956	Robinson (SWAC)
95	61	58	1957	Robinson (SWAC)
9	67	63	1956	Robinson (SWAC)
5	75	73	1906	Morehead
425	79	77	1957	Robinson, Selfridge (SWAC)
271	84	81	1957	Robinson, Selfridge (SWAC)
7	120	117	1956	Robinson (SWAC)
5	127	125	1956	Robinson (SWAC)
17	147	144	1956	Robinson (SWAC)
1575	157	150	1956	Robinson (SWAC)
3	209	207	1956	Robinson (SWAC)
15	229	226	1956	Robinson (SWAC)
29	231	228	1956	Robinson (SWAC)
403	252	250	1957	Robinson, Selfridge (SWAC)
177	271	267	1957	Robinson, Selfridge (SWAC)
21	276	268	1956	Robinson (SWAC)
7	290	284	1956	Robinson (SWAC)
7	320	316	1956	Robinson (SWAC)
27	455	452	1956	Robinson (SWAC)
5	1947	1945	1957	Robinson (SWAC)

THEOREM. *A prime of the form* $N=3\cdot 2^n+1$, *where* n *is even, cannot be a factor of any Fermat number.*

PROOF. The condition that 2 should be a cubic residue mod N, for any prime $N\equiv 1 \pmod 6$, is that in the unique representation of N in the form $N=A^2+3B^2$, the number B should be a multiple of 3. (See, for example, Friedman and Hall [4].) Now, in the present case, $A=1$ and $B=2^{n/2}$, so that 2 is not a cubic residue. Hence, as previously noted, N cannot be a factor of any Fermat number.

Actually, the residue of $2^{2^{n-2}} \pmod N$ was computed in this case also, and, curiously enough, this was the only case noticed where the residue had an interesting form without being ± 1. It is, in fact, easy to verify that if $N=3\cdot 2^n+1$ is prime, and $n>2$ is even, then

$$2^{2^{n-2}} \equiv 3(\pm 2^{n-1} \pm 2^{(n/2)-1}) \pmod N,$$

with some combination of signs. It may be of interest to record the signs actually obtained. For the eleven even values of n with $2<n<1280$ for which $N=3\cdot 2^n+1$ is prime, the signs in the above congruence were as follows:

$+\ +$ for $n = 276$; $\quad -\ +$ for $n = 6, 18, 66, 438, 534$;

$+\ -$ for $n = 30$; $\quad -\ -$ for $n = 8, 12, 36, 408$.

The first sign being plus is found to correspond to 2 being a quartic residue mod N. It is not clear why this case should be unusual.

Added in proof. It follows from a recent unpublished result of Emma Lehmer that the two signs will be like if $n\equiv 0 \pmod 4$ and unlike if $n\equiv 2 \pmod 4$.

REFERENCES

1. A. J. C. Cunningham, *Quadratic and linear tables*, London, F. Hodgson, 1927.

2. A. J. C. Cunningham and H. J. Woodall, *Factorisation of* $Q=(2^q\mp q)$ *and* $(q\cdot 2^q\mp 1)$, Messenger of Mathematics vol. 47 (1917) pp. 1–38.

3. L. E. Dickson, *History of the theory of numbers*, vol. 1, Washington, Carnegie Institution, 1919.

4. B. Friedman and M. Hall, *Solutions to Problem* 3707, Amer. Math. Monthly vol. 44 (1937) pp. 397–400.

5. M. Kraitchik, *Recherches sur la théorie des nombres*, vol. 1, Paris, Gauthier-Villars, 1924.

6. ———, *Théorie des nombres*, vol. 2, Paris, Gauthier-Villars, 1926.

7. J. C. Morehead, *Note on the factors of Fermat's numbers*, Bull. Amer. Math. Soc. vol. 12 (1906) pp. 449–451.

8. H. Riesel, *A note on the prime numbers of the forms* $N=(6a+1)2^{2n-1}-1$ *and* $M=(6a-1)2^{2n}-1$, Ark. Mat. vol. 3 (1956) pp. 245–253.

9. ———, *A new Mersenne prime*, Math. Tables Aids Comput. vol. 12 (1958) p. 60.

10. R. M. Robinson, *Mersenne and Fermat numbers*, Proc. Amer. Math. Soc. vol. 5 (1954) pp. 842–846.

11. ———, *Factors of Fermat numbers*, Math. Tables Aids Comput. vol. 11 (1957) pp. 21–22.

12. ———, *Table of factors of numbers one unit larger than small multiples of powers of two*, Paris, Gauthier-Villars, 1957. (Tabulated)

13. ———, *Some factorizations of numbers of the form* $2^n \pm 1$, Math. Tables Aids Comput. vol. 11 (1957) pp. 265–268.

14. ———, *The converse of Fermat's theorem*, Amer. Math. Monthly vol. 64 (1957) pp. 703–710.

15. P. Seelhoff, *Die Zahlen von der Form* $k \cdot 2^n + 1$, Zeitschrift für Mathematik und Physik, vol. 31 (1886) p. 380.

16. J. L. Selfridge, *Factors of Fermat numbers*, Math. Tables Aids Comput. vol. 7 (1953) pp. 274–275.

UNIVERSITY OF CALIFORNIA, BERKELEY