Concerning the Numbers $2^{2p} + 1$, p Prime

By John Brillhart

1. Introduction. In a recent investigation [7] the problem of factoring numbers of the form $2^{2p} + 1$, p a prime, was encountered. Since $2^{2p} + 1 = (2^p - 2^{\frac{1}{2}(p+1)} + 1)(2^p + 2^{\frac{1}{2}(p+1)} + 1)$ for odd p, the problem consists of factoring the two trinomials on the right. In this paper the results of a search for factors of these trinomials are given, as well as a determination of the nature of certain of these numbers for which no factor was found.

2. Elementary factors. Let $N_p = (2^p - 2^{\frac{1}{2}(p+1)} + 1)(2^p + 2^{\frac{1}{2}(p+1)} + 1) = A_p \cdot B_p$, p an odd prime.

A. From the fact that $5 \mid N_p$, it easily follows that $5 \mid A_p$ iff $p \equiv \pm 1 \pmod 8$ and $5 \mid B_p$ iff $p \equiv \pm 3 \pmod 8$. On the other hand, $5^2 \nmid N_p$ unless $p = 5$; for, since 2 is a primitive root of 25, 2 belongs to the exponent $\phi(25) = 20$. But $2^{2p} \equiv -1 \pmod{25}$, or $2^{4p} \equiv 1 \pmod{25}$. Therefore, $20 \mid 4p$, or $p = 5$. Thus, if $p = 5$, $5^2 \mid 2^{10} + 1 = 1025$, while if $p \neq 5$, $5^2 \nmid N_p$.

B. If q is a prime $\neq 5$ and $q \mid N_p$, then $2^{4p} \equiv 1 \pmod q$. But then 2 belongs to the exponent $4p \pmod q$. Thus by Fermat's Theorem, $4p \mid q - 1$; that is, every prime divisor $\neq 5$ of A_p or B_p is $\equiv 1 \pmod{4p}$.

C. Suppose p is odd and $q = 4p + 1$ is a prime. Then $2^{q-1} = 2^{4p} \equiv 1 \pmod q$. It follows from Euler's Criterion that $2^{2p} \equiv \left(\frac{2}{q}\right) \pmod q$. But since p is odd, $q \equiv 5 \pmod 8$. Therefore, $2^{2p} \equiv -1 \pmod q$, or $q \mid 2^{2p} + 1$. Unfortunately, however, it has not been possible to discover the conditions that determine which of A_p and B_p q will divide.

3. The Search.

A. *Extent.* The search for prime factors $q \neq 5$ of A_p and B_p, which was conducted on the IBM 701 at the University of California, Berkeley, was made over the following intervals:

$$1 < q < \sqrt{B_{59}} \quad \text{for} \quad B_{59}$$
$$1 < q < 3 \cdot 2^{30} \quad \text{for} \quad A_{71}$$
$$1 < q < 2^{30} \quad \text{for} \quad 71 < p \leqq 179 \text{ and } p = 241$$
$$1 < q < 2^{28} \quad \text{for} \quad 179 < p < 1200, p \neq 241.$$

No N_p for $p < 71$, $p \neq 59$, were considered, since these numbers have been completely factored. N_{241} was examined along with N_{73} to the bound 2^{30}, these numbers being of particular interest (See [7]).

B. *Results.* (i) The program produced a vast number of new factors, as well as several corrections to the literature (See [4]). The new factors of N_p, $p < 250$, are indicated in the accompanying table by * to distinguish them from factors pre-

Received January 10, 1962.

viously known [2]. For $250 < p < 1200$ all factors $> 300{,}000$ are new, and are therefore not indicated by *. A dot following the final factor means that the nature of the complementary factor is unknown.

(ii) A complete factorization was accomplished for B_{59}, A_{83}, and A_{103}, the primality of the complementary factor in each case being assured by the non-existence of a factor below its square root. The factorization of B_{59} is of particular interest, since this number appears in [2] and [3] as a prime.

The author would like to thank Mr. K. R. Isemonger for providing the complete factorization of B_{97}, as well as the much sought after factorization for A_{71}, which, previous to his attack on the number, had only been known to factor into the product of two primes.

(iii) A program was written to test the divisibility and multiplicity of all known factors, with the result that all factors were found to be correct, but none was found to be multiple.

C. *The Program.* The structure of the search program was similar to that described in [1]. In particular, for each p a table of differences was computed from the first $1155 = 3 \cdot 5 \cdot 7 \cdot 11$ terms of the sequence $4pk + 1$, $k = 1, 2, \cdots$, that remained after the multiples of 3, 5, 7, and 11 had been sieved out. This table was used repeatedly by the program to produce a sequence of trial divisors, among which the factors, if any, were to be found. The remainders of A_p and B_p for each trial divisor were calculated by residue methods, both remainders being calculated at the same time because of the similarity in form of A_p and B_p. The occurrence of a 0 remainder in this calculation signalled the discovery of a factor of one of the two numbers, but not both, since obviously they are relatively prime. To examine each N_p required from 5 to 15 minutes, the N_p for the larger p's requiring a shorter time.

4. Primality Testing.

A. At the conclusion of the search for factors, the primality of several numbers of immediate interest, namely, A_{73} and A_{241}, was still in doubt, because no factor had been found. It was then noted by Professor D. H. Lehmer that the primality of numbers of the form under consideration could be decided by Proth's Theorem [5]: "If $M = k \cdot 2^n + 1$, where $0 < k < 2^n$, and $\left(\frac{a}{M}\right) = -1$, then M is prime iff $a^{\frac{1}{2}(M-1)} \equiv -1 \pmod{M}$." In the present case A_p, $B_p = M = (2^{\frac{1}{2}(p-1)} \pm 1) \cdot 2^{\frac{1}{2}(p+1)} + 1$, with $0 < k = 2^{\frac{1}{2}(p-1)} \pm 1 < 2^{\frac{1}{2}(p+1)}$ for p an odd prime, the value of a being easily obtained from the reciprocity law for the Jacobi symbol.

A program was accordingly written by Professor Lehmer for the IBM 701 to calculate the required residues. The modulus used for each test was N_p rather than the A_p or B_p in question, so that the reduction of the successive powers could be accomplished by multi-precision subtraction instead of division by a multi-precision divisor. The remainder thus produced was further reduced mod A_p or B_p by a subtractive routine written by the author. The final residues in binary from both routines have been preserved on IBM cards for later checking purposes.

B. It is believed that the two testing programs were accurate, since the anticipated results were obtained in every trial case save one. In this case, B_{59}, a discrepancy existed between the literature, which stated the number was prime, and the

TABLE OF FACTORS

p	$2^p - 2^{\frac{1}{2}(p+1)} + 1$	$2^p + 2^{\frac{1}{2}(p+1)} + 1$
3	5	13
5	5^2	41
7	113	5·29
11	5·397	2113
13	5·1613	53·157
17	137·953	5·26317
19	5·229·457	525313
23	277·30269	5·1013·1657
29	5·107367629	536903681
31	5581·384773	5·8681·49477
37	5·149·184481113	593·231769777
41	181549·12112549	5·10169·43249589
43	5·1759217765581	173·101653·500177
47	140737471578113	5·3761·7484047069
53	5·1801439824104653	15358129·586477649
59	5·1181·3541·157649·174877	5521693*·104399276341*
61	5·733·1709·368140581013	3456749·667055378149
67	5·269·42875177·2559066073	15152453·9739278030221
71	4999465853·472287102421	5·569·148587949·5585522857
73	prime	5·293·9929·649301712182209
79	prime	5·317·
83	5·13063537*·148067197374074653*	997·
89	1069·	5·
97	389·4657·	5·3881·5821·3555339061·394563864677
101	5·	809·
103	41201·520379897*·473000157711296729*	5·17325013*·
107	5·857·	843589·
109	5·	5669·666184021*·
113	prime	5·58309·2362153*·
127	509·26417·140385293*·	5·18797·72118729*·
131	5·642811237*·	269665073*·
137	189061·	5·
139	5·1408349*·	557·
149	5·	1789·
151	prime	5·
157	5·	prime
163	5·653·9781·7807049*·	prime
167	prime	5·75005713*·
173	5·	c
179	5·31815461*·	c
181	5·9413·	c
191	25212001*·	5·3821·
193	773·	5·3089·148997·
197	5·4729·	52009·
199	797·	5·
211	5·95110361*·	c
223	95768689*·	5·11597·6530333*·
227	5·	54449·83132849*·

TABLE OF FACTORS—*Continued*

p	$2^p - 2^{\frac{1}{2}(p+1)} + 1$	$2^p + 2^{\frac{1}{2}(p+1)} + 1$
229	5·2749·5523481*·	c
233	30757·	5·3108221*·
239	prime	5·
241	prime	5·2640397*·15594629*·
251	5·1912621·	5021·
257	c	5·28564009·
263	c	5·119929·731141·
269	5·2153·3229·5381·4273873·	8609·
271	10474693·	5·97561·
277	5·1109·	232681·98002601·
281	91568909·	5·3373·3827221·
283	5·	prime
293	5·22396921·	5861·12893·60488093·
307	5·93329·1021697·	1229·7369·254197·201846361·
311	6221·21149·	5·
313	42569·681089·6386453·	5·
317	5·	c
331	5·589181·	c
337	683437·30499849·	5·5393·32353·2549069·
347	5·5575597·60988721·	2777·
349	5·8377·763613·	c
353	prime	5·
359	585889·5199757·	5·
367	prime	5·
373	5·1493·	c
379	5·4549·10219357·	prime
383	13789·111650629·	5·4597·
389	5·17117·51349·2852149·	c
397	5·11117·	14293·25409·6312301·
401	c	5·3209·
409	1637·9817·	5·4909·1531297·1856861·
419	5·63689·356989·	53633·186037·
421	5·31142213·	c
431	91373·3754873·	5·
433	1733·5197·	5·31177·239017·
439	695377·	5·
443	c	5·
449	3615349·111190361·	5·3593·165233·
457	prime	5·71293·
461	5·14753·7278269·	226813·21102737·
463	c	5·46475941·
467	5·13453337·	252181·1372981·
479	6380281·39557737·79190197·	5·70309537·
487	1949·	5·7793·890237·
491	5·	3929·34631213·
499	5·43913·1179637·	1997·
503	6037·10061·	5·
509	5·103837·	4073·13350053·
521	c	5·16673·
523	5·8369·351457·	c

TABLE OF FACTORS—*Continued*

p	$2^p - 2^{\frac{1}{2}(p+1)} + 1$	$2^p + 2^{\frac{1}{2}(p+1)} + 1$
541	5·1281089·10393693·	262302769·
547	5·67887077·	c
557	5·	c
563	5·	51797·133489553·
569	37690561·	5·47797·170701·257189·
571	5·2384497·5536417·94600997·	c
577	2309·92936237·	5·
587	5·35221·	13658317·
593	c	5·
599	306689·9385133·	5·4793·86257·
601	7213·	5·79333·685141·
607	c	5·
613	5·	17458241·
617	c	5·86381·
619	5·114519953·	2477·103993·284741·
631	c	5·328121·651193·
641	c	5·62248793·
643	5·	c
647	144563093·	5·854041·9679121·
653	5·	c
659	5·5273·	1534153·
661	5·	c
673	2693·26921·419953·4118761·	5·
677	5·5417·	c
683	5·	c
691	5·	11057·
701	5·	c
709	5·	2837·
719	c	5·8629·
727	2909·	5·
733	5·	627449·
739	5·523213·170756297·	2957·6139613·
743	260683037·	5·
751	c	5·9013·
757	5·	c
761	82189·529657·1567661·	5·9133·
769	c	5·
773	5·9277·961613·8979169·28764877·	
787	5·	47221·406093·14121929·
797	5·	
809		5·6473·25889·1948073·
811	5·	5336381·
821	5·	
823	19753·17678041·	5·
827	5·36389·148861·2312293·	
829	5·	
839	5564249·	5·
853	5·3413·	
857		5·

TABLE OF FACTORS—*Continued*

p	$2^p - 2^{\frac{1}{2}(p+1)} + 1$	$2^p + 2^{\frac{1}{2}(p+1)} + 1$
859	5·82488053·	41233·18970157·
863	62137·	5·
877	5·136813·	178909·
881	292493·	5·
883	5·3533·10597·	
887		5·
907	5·	
911	109321·	5·29153·
919	15174529·	5·3677·169097·
929	11149·319577·	5·7433·85469·858397·
937		5·802073·
941	5·3383837·	
947	5·189401·	6522937·
953		5·
967	328781·12056557·	5·47054221·
971	5·	19421·
977		5·
983		5·
991	47569·	5·27749·
997	5·3989·23929·1316041·	
1009	12109·	5·242161·
1013	5·33449261·	
1019	5·61141·207877·	
1021	5·	88557457·
1031	181457·	5·32993·
1033		5·4133·78509·
1039	4157·47577889·	5·
1049	4640777·	5·
1051	5·92489·2030533·	1513441·77933753·
1061	5·49459577·	
1063	4253·119057·2351357·	5·
1069	5·25657·	
1087		5·4349·182617·
1091	5·13093·	
1093	5·13155349·	4373·
1097		5·114089·79321877·
1103	132361·	5·525029·
1109	5·13309·	115337·
1117	5·67021·	40213·71514809·
1123	5·40429·	4493·597437·
1129		5·4517·
1151		5·36833·
1153	152197·67796401·	5·
1163	5·37217·37453253·	
1171	5·13152673·	
1181	5·	1369961·9178733·
1187	5·9497·151937·	
1193		5·

test routine, which stated the opposite. The number was immediately run on the factoring program, and much to the satisfaction of all concerned, a factor was found, and the test routine was exonerated.

A further verification of a kind has come from Mr. Isemonger, who, acting on the test results that A_{71} and B_{97} were composite, succeeded in finding the factorizations mentioned above.

C. All A_p and B_p, $71 \leqq p \leqq 757$, for which no elementary or other factor was known, were tested for primality. In all, 50 numbers were tested, with the result that 14 of them were found to be prime. These are listed as prime in the accompanying table, while the remaining 36 composite numbers are indicated as such by a "c" in the proper positions of the table.

Each number with $71 \leqq p \leqq 457$ was tested twice with complete agreement in the results. No number for $p > 457$ was tested twice, for testing a single number in this range required approximately 30 minutes.

5. Acknowledgements. The author would like to express his gratitude to Professor Lehmer for his very generous contributions of time and effort in constructing the primality test, which has brought this paper to such a satisfactory conclusion. In addition, he would like to thank Dr. John Selfridge for his careful reading of the preliminary manuscript, and Mr. Vance Vaughan and Robert Innes for their assistance in the production phase of the program.

University of San Francisco
San Francisco, California

1. John Brillhart & G. D. Johnson, "On the factors of certain Mersenne numbers," *Math. Comp.*, v. 14, 1960, p. 365–369.

2. A. J. C. Cunningham & H. J. Woodall, *Factorizations of* $(y^n \mp 1)$, Hodgson, London, 1925, p. 6–9.

3. M. Kraitchik, *Recherches sur la Théorie des Nombres*, Tome II, Paris, 1929.

4. D. H. Lehmer, *Guide to the Tables in the Theory of Numbers*, National Research Council Bulletin, Washington, 1941, p. 29–30, 135–136.

5. F. Proth, "Théorèmes sur les nombres premiers," *C. R. Acad. Sci. Paris*, v. 87, 1878, p. 926.

6. R. M. Robinson, "Some factorizations of numbers of the form $2^n \pm 1$," *MTAC*, v. 11, 1957, p. 265–268.

Robert Spira, "The complex sum of divisors," *Amer. Math. Monthly*, v. 68, 1961, p. 120–124.