incomplete Burnett type coefficients of powers of z^{-1} higher than the fourth. Above about $z = 10$ it is also evident that for a computer carrying only twelve figures there is nothing to be gained in using a more elaborate converging factor than $R_p/u_p = 0.5$.

National Research Council of Canada
Ottawa, Canada

1. E. Dempsey & G. C. Benson, "Tables of the modified Bessel functions of the second kind for particular types of argument," *Can Jn. Phys.*, v. 38, 1960, p. 399. This paper contains tables of $K_n\left(\frac{\pi}{2}\sqrt{q}\right)$ for $q = 1(1.0)\,250$ and of $K_n\left(\frac{\pi}{3}\sqrt{q}\right)$ for $q = 1(1.0)\,300$. In both cases values for integral orders 0 to 10 were computed to ten significant figures.
2. R. B. Dingle, "Asymptotic expansions and converging factors. I. General theory and basic converging factors," *Proc.*, Roy. Soc., London, v. 244A, 1958, p. 456.
3. R. B. Dingle, "Asymptotic expansions and converging factors. IV Confluent hypergeometric, parabolic cylinder, modified Bessel, and ordinary Bessel functions," *Proc.*, Roy. Soc., London, v. 249A, 1959, p. 270.
4. D. Burnett, "The remainders in the asymptotic expansions of certain Bessel functions," *Proc.*, Camb. Phil. Soc., v. 26, 1930, p. 145.
5. E. Jahnke & F. Emde, *Tables of Functions*, Fourth Edition, Dover, New York, 1945, p. 138.
6. W. S. Aldis, "Tables for the solution of the equation $\frac{d^2y}{dx^2} + \frac{1}{x}\cdot\frac{dy}{dx} - \left(1 + \frac{n^2}{x^2}\right)y = 0$," *Proc.*, Roy. Soc., London, v. 64, 1899, p. 203.

On the Factors of Certain Mersenne Numbers

By John Brillhart and G. D. Johnson

1. Introduction. For the past 10 months the authors have been conducting a search for factors of certain Mersenne numbers on the IBM 701 at the Computer Center, University of California, Berkeley. The following is a report on the nature and results of that search.

2. Extent. Prime factors q were sought for the numbers $M_p = 2^p - 1$ for primes $p < 1200$ in the intervals indicated:

$p = 101$		$2^{30} < q < 2^{35}$
$103 \leqq p \leqq 157,$	$p \neq 151$	$2^{30} < q < 2^{31}$
$157 < p \leqq 257$		$1 < q < 2^{31}$
$257 < p \leqq 1021,$	$p \neq 397$	$1 < q < 2^{30}$
$p = 397$		$1 < q < 2^{32}$
$1021 < p < 1200$		$1 < q < 2^{28}$

No factors $<2^{30}$ were examined for $101 \leqq p \leqq 157$, since these had already been investigated [1]. No M_p were examined for $p < 101$ or $p = 151$, since these numbers have presumably been completely factored. Possible factors $<2^{35}$ were

Received May 5, 1960.

also investigated for M_{65537}, the Mersenne number whose exponent is the "last" Fermat prime. M_{397} was investigated to 2^{32} in the hope of finding more small factors.

3. Results.

A. Fifty-five new prime factors were discovered, 6 of which for M_p below the traditional "limit" $p = 257$. These factors are given in the accompanying table, and are indicated by *. Also included are all published prime factors, and 6 new ones (indicated by †) of E. Karst, Brigham Young University. Thus, the table is believed to be a complete listing of all prime factors of M_p for $p < 1200$ known at this time. No factor was found for M_{65537}, whose character is still unknown. Since no factor was found to M_{101} below its cube root, it is the product of two primes.

B. All known prime factors of M_n, $n < 10\ 000$, were tested and found correct, with the exception of the two misprints in H. Riesel [2], as noted earlier by J. Selfridge [3]. In addition, all factors were tested for multiplicity, but no new multiple factors appeared. Hence, to date, only a few multiple factors are known for composite exponents n, while none have been found for prime exponents, further supporting the conjecture that none exist.

4. The Program.

A. STRUCTURE. If $d \mid M_p$, then $d \equiv 1 \pmod{2p}$. Also, since 2 is a quadratic residue of M_n, n odd, then $d \equiv \pm 1 \pmod 8$. Thus, the divisors, d, lie among the common terms t_n of these arithmetic sequences.

In production these terms were generated consecutively by the repeated use of an increment table, which had also been constructed to produce no terms divisible by 3, 5, 7, or 11. (See [1].)

Divisibility of M_p by each t_n was tested by examining the remainder of M_p (mod t_n) for 0.

For $101 \leqq p \leqq 223$, M_p was reduced mod t_n by multiple precision division.

Example 1. The remainder of M_{101} mod t_n was computed for each t_n by 3 divisions, until t_n was $>2^{31}$, at which time an initial dividend of 67 binary places could be used. This change, which produced the remainder in only 2 divisions, was actually introduced when t_n was $>2^{28}$ by using a modulus of $2^{\alpha}t_n$, $0 < \alpha \leqq 3$, instead of t_n, the error in the final remainder being removed after the last division by an appropriate number of subtractions of t_n, or multiples of t_n. This device was used consistently in all routines whenever possible.

When the program was first run for $p \geqq 223$, the final remainder was computed by residue methods consisting of successive squarings and doublings of the residue of some initial power of 2, followed by a subtraction of 1. Later it was realized, that in a double register machine like the 701, a residue between the initial and final residue could usually be multiplied by a power of 2 greater than the first without producing an illegal divide condition in the registers. The magnitude of the power that could be used was found to depend on the length of the registers (35 binary places) and the length of t_n.

This discovery decreased the testing time for each t_n by about 30%, but greatly complicated the programming, since from the many possible programs, one had to be chosen that required a minimum number of machine cycles.

TABLE OF FACTORS

p	*Factors*	*p*	*Factors*
2	3	227	
3	7	229	1504073·20492753*·
5	31	233	1399·135607·622577·
7	127	239	479·1913·5737·176383·134000609*·
11	23·89	241	22000409*·
13	8191	251	503·54217·
17	131071	257	
19	524287	263	23671·
23	47·178481	269	13822297*
29	233·1103·2089	271	
31	2147483647	277	1121297·
37	223·616318177	281	80929·
41	13367·164511353	283	9623·
43	431·9719·2099863	293	
47	2351·4513·13264529	307	14608903*·85798519*·
53	6361·69431·20394401	311	5344847·
59	179951·3203431780337	313	10960009*·
61	2305843009213693951	317	9511·
67	193707721·761838257287	331	
71	228479·48544121·212885833	337	18199·2806537†·
73	439·2298041·9361973132609	347	
79	2687·202029703·1113491139767	349	
83	167·57912614113275649087721	353	931921·
89	618970019642690137449562111	359	719·855857·778165529*·
97	11447·prime	367	12479·51791041*.
101		373	25569151*·
103		379	
107	prime	383	1440847·
109	745988807·	389	56478911*·
113	3391·23279·65993·1868569 ·1066818132868207	397	2383·6353·50023·53993 ·202471·5877983†·
127	prime	401	
131	263·	409	
137		419	839·
139		421	
149		431	863·3449·36238481*·76859369* ·558062249*·
151	18121·55871·165799·2332951·prime		
157	852133201·	433	
163	150287·704161·110211473*·	439	104110607*·
167	2349023·	443	887·
173	730753·1505447·	449	1256303·
179	359·1433·	457	150327409*·
181	43441·1164193·7648337*·	461	2767·
191	383·	463	11113·3407681†·
193	13821503*·	467	121606801*·
197	7487·	479	33385343*·
199		487	4871·
211	15193·	491	983·7707719†·
223	18287·196687·1466449·2916841·	499	20959·

Table of Factors—*Continued*

p	*Factors*	*p*	*Factors*
503		839	26849·
509	12619129†·	853	
521	prime	857	6857·
523		859	7215601·
541		863	8258911·169382737*·
547	5471·	877	35081·1436527*·
557	3343·21993703*·	881	26431·
563		883	8831·63577*·
569	15854617*·55470673*·	887	16173559*·
571	5711·27409*·	907	1170031·
577	3463·	911	1823·26129303*·
587	554129·2926783*·	919	
593	104369·	929	13007·
599		937	28111·
601	3607·64863527*·	941	7529·
607	prime	947	295130657*·
613		953	343081·
617	59233·	967	23209·549257*·
619	110183·	971	
631		977	867577·1813313*·
641	35897·49999*·	983	
643	3189281·	991	
647		997	
653	78557207*·289837969*·	1009	3454817·
659	1319·	1013	6079·
661		1019	2039·75407*
673	581163767*·	1021	40841·795808241*·
677		1031	2063·435502649*·
683	1367·	1033	196271·36913223*·
691		1039	5080711·
701	796337·2983457*·28812503*·	1049	33569·459463*·
709	216868921*·	1051	3575503·
719	1439·772207*·	1061	
727		1063	
733		1069	
739		1087	10722169*·
743	1487·	1091	87281·
751		1093	43721·111487*·
757	9815263·561595591*·	1097	980719·4666639*·
761	4567·6089*·	1103	2207·
769		1109	
773	6864241·9461521†·	1117	53617·
787		1123	
797		1129	33871·
809		1151	
811	326023·	1153	267497·
821	419273207*·	1163	
823		1171	
827	66161·	1181	4742897·
829	72953·	1187	256393·113603023*·
		1193	121687·

In some cases, the initial residue was produced from a comparatively small power of 2 by a single division, while in others, it was obtained from a fairly large power of 2 by multiple-precision division.

Example 2. For M_{397}, 4 different programs were used, each improving on and replacing the preceding, when the length of t_n permitted. The first divisor used was $t_1 = 3 \cdot 794 + 1 = 2383$, which also happens to be the first factor. This is shown below by the calculation schemes of the 4 programs, although only the first was actually used to test such a small possible divisor. With each scheme is also given the interval of t_n, for which it was used. The letters *ir* after a residue indicate the initial residue used by the squaring part of the routine.

I: $1 < t_n < 2^{25}$.	II: $2^{25} < t_n < 2^{27}$.	III: $2^{27} < t_n < 2^{29}$.	IV: $2^{29} < t_n < 2^{32}$.
$2^{25} \equiv 1792 \pmod{2383}$	$2^{60} \equiv 1657 \pmod{2383}$	$2^{62} \equiv 1862 \pmod{2383}$	$2^{64} \equiv 299 \pmod{2383}$
$2^{60} \equiv 1657$	$2^{95} \equiv 342$ *ir*	$2^{97} \equiv 1368$ *ir*	$2^{99} \equiv 706$ *ir*
$2^{95} \equiv 342$ *ir*	$2^{190} \equiv 197$	$2^{194} \equiv 769$	$2^{198} \equiv 389$
$2^{190} \equiv 197$	$2^{196} \equiv 693$	$2^{197} \equiv 1386$	$2^{396} \equiv 1192$
$2^{196} \equiv 693$	$2^{392} \equiv 1266$	$2^{394} \equiv 298$	$2^{397} \equiv 1$
$2^{392} \equiv 1266$	$2^{397} \equiv 1$	$2^{397} \equiv 1$	
$2^{397} \equiv 1$			

B. PRODUCTION. The program was run for 60 hours, each $p < 223$ requiring approximately 23 minutes, and each $p \geqq 223$ requiring from 8 to 18 minutes, the larger exponents taking progressively less time. The special number M_{101} was run for 10 hours.

The routines used are believed to have been accurate, a fact which will be ascertained at a future time, when more rapid computers will accomplish in a few minutes, what has now taken many hours.

The authors would like to thank Professors R. M. Robinson and D. H. Lehmer for their suggestions and ideas, and also the staff of the Computer Center for their many courtesies.

University of California
Richmond, California

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

———— "Mersenne and Fermat numbers," Amer. Math. Soc. *Proc.*, v. 5, 1954, p. 842–846.

2. H. RIESEL, "Mersenne numbers," *MTAC*, v. 12, 1958, p. 207–213.

3. J. L. SELFRIDGE, Table Errata, *MTAC*, v. 13, 1959, p. 142.