File Copy

BRL R 1300

BRL

AD [illegible]

REPORT NO. 1300

PRIMALITY OF A CERTAIN CLASS OF INTEGERS

by

Lynn S. Mohler

August 1965

U. S. ARMY MATERIEL COMMAND
BALLISTIC RESEARCH LABORATORIES
ABERDEEN PROVING GROUND, MARYLAND

B A L L I S T I C   R E S E A R C H   L A B O R A T O R I E S

REPORT NO. 1300

AUGUST 1965

PRIMALITY OF A CERTAIN CLASS OF INTEGERS

Lynn S. Mohler

Computing Laboratory

RDT & E Project No. 1P014501A14B

A B E R D E E N   P R O V I N G   G R O U N D,   M A R Y L A N D

BALLISTIC RESEARCH LABORATORIES

REPORT NO. 1300

LSMohler/bj
Aberdeen Proving Ground, Md.
August 1965

PRIMALITY OF A CERTAIN CLASS OF INTEGERS

ABSTRACT

This report is concerned with determining the primeness of the members of a class of numbers of the form, $B_p = \frac{2^p + 1}{3}$, where p is an odd prime. This class is similar to the Mersenne and Fermat numbers. A theorem is proven which characterizes the factors of B_p. This study was conducted using BRLESC, the high-speed digital computer at BRL and a description is given of the program used. Finally, the B_p's that were found to be prime as well as the B_p's that were found to be composite are tabulated.

The Mersenne numbers, which have the general form $M_p = 2^p - 1$, and the family of numbers, the Fermat numbers, which have the form $F_p = 2^p + 1$, have been studied for centuries. Just recently a renewed interest in them has been brought about by the use of the high-speed computers (see, for example, [3]*).

Since the Fermat numbers cannot be prime unless p is a power of two (i.e., unless $p = 2^m$ for some integer m), the Fermat numbers have been defined as $F_m = 2^{2^m} + 1$ and this is the form in which they have been investigated. To see that F_p is composite when p is not a power of two, first note that a power of two cannot have any odd factors. Hence, if p is not a power of two, we can write p = rs, where s > 1 is odd. Using the fact that when m is odd

$$x^m + y^m = (x + y)(x^{m-1} - x^{m-2}y + x^{m-3}y^2 - \dots - xy^{m-2} + y^{m-1}) \quad ,$$

we substitute $x = x^n$, $y = y^n$ obtaining

$$x^{mn} + y^{mn} = (x^n + y^n)(x^{n(m-1)} - x^{n(m-2)}y^n + x^{n(m-3)}y^{2n} - \dots - x^n y^{n(m-2)} + y^{n(m-1)}) \quad .$$

Therefore, we have

$$2^p + 1 = 2^{rs} + 1 = (2^r + 1)(2^{r(s-1)} - 2^{r(s-2)} + 2^{r(s-3)} - \dots - 2^r + 1)$$

which shows that F_p has a factor of $2^r + 1$.

This paper is concerned with the case of p equal to an odd prime, so that

$$2^p + 1 = (2 + 1)(2^{p-1} - 2^{p-2} + 2^{p-3} - \dots - 2 + 1)$$

$$2^p + 1 = 3\left[(2^{p-1} - 2^{p-2}) + (2^{p-3} - 2^{p-4}) + \dots + (2^2 - 2) + 1\right]$$

$$2^p + 1 = 3\left[2^{p-2}(2 - 1) + 2^{p-4}(2 - 1) + \dots + 2(2 - 1) + 1\right]$$

$$2^p + 1 = 3(2^{p-2} + 2^{p-4} + \dots + 2 + 1) \quad .$$

* *Numbers in brackets refer to references found on page 20.*

Clearly, F_p always has a factor of 3 when p is an odd prime. This gives rise to the definition of a new family of numbers, B_p, where p is an odd prime and

$$B_p = \frac{2^p + 1}{3} .$$

The following two lemmas are used in the proof of theorem I and this result is utilized in determining the primeness of B_p.

Lemma 1: $M_p \equiv 1 \pmod{p}$, for any odd prime p.

Proof: By Fermat's theorem, $2^{p-1} \equiv 1 \pmod{p}$ or $2^p \equiv 2 \pmod{p}$, [2, p. 277]. Subtracting one from both sides, we have $2^p - 1 \equiv 1 \pmod{p}$.

Lemma 2: $B_p \equiv 1 \pmod{p}$, for any prime $p > 3$.

Proof: Adding $2^p \equiv 2 \pmod{p}$ and $1 \equiv 1 \pmod{p}$, we obtain $2^p + 1 \equiv 3 \pmod{p}$. Since $2^p + 1$ has a factor of 3 and the greatest common divisor of p and 3 is 1 whenever $p > 3$ and p is prime, it follows that

$$B_p = \frac{2^p + 1}{3} \equiv 1 \pmod{p}, \text{ [2, p. 223]} .$$

<u>Theorem I</u>. If B_p is composite with prime factor q and p is a prime greater than 3, then q must be of the form $q = 2kp + 1$ for some $k = 1, 2, 3, \ldots$.

Proof: By D. H. Lehmer's Law of Apparition, it follows that p is some divisor of $q - \sigma\epsilon$, where $B_p \equiv \epsilon \pmod{p}$ and $M_p \equiv \sigma \pmod{p}$, see [1]. By the previous lemmas, $\epsilon = \sigma = 1$. Therefore, $q - 1 = k'p$ for some k'. Since B_p is odd, q must also be odd. Consequently, $k'p$ is even; and since p is an odd prime, k' must be even. We can therefore set $k' = 2k$ for some integer k and hence q is of the form $q = 2kp + 1$.

<u>Theorem II</u>. If k in theorem I is odd, then q is of the form $q = 8n + 3$; and if k is even, then q is of the form $q = 8n + 1$, for some integer n.

Proof: Since $q = 2kp + 1$,

$$\frac{q-1}{2} = k\,p .$$

Euler's Criterion states that if $2^{\frac{q-1}{2}} \equiv 1 \pmod{q}$, then 2 is a quadratic residue of a prime q; and if $2^{\frac{q-1}{2}} \equiv -1 \pmod{q}$, then 2 is a non-residue of a prime q, [4, p. 203].

Case A. k is even. In this case,

$$2^{\frac{q-1}{2}} = 2^{kp} = (2^p)^k \equiv (-1)^k \equiv 1 \pmod{q} .$$

Hence by Euler's Criterion, 2 is a quadratic residue of q. By induction, $q = 8n + 1$ or $q = 8n + 7$, see [4, p. 278]. Since, by theorem I, we know $q = 2kp + 1$, $q \neq 8n + 7$ for any n. Therefore, $q = 8n + 1$ for some integer n.

Case B. k is odd. Now, $(-1)^k = -1$ and hence

$$2^{\frac{q-1}{2}} = 2^{kp} = (2^p)^k \equiv (-1)^k \equiv -1 \pmod{q} .$$

2 is therefore a non-residue of a prime q. By induction, $q = 8n + 3$ or $q = 8n + 5$ for some integer n, [4, p. 278]. Again, since $q = 2kp + 1$, $q \neq 8n + 5$ for any n. Hence $q = 8n + 3$ for some n.

Using BRLESC, the high-speed digital computer of the Ballistic Research Laboratories, a program was written to determine the primeness of B_p for odd prime numbers p. This was accomplished by dividing by all possible divisors of the form $q = 2kp + 1$. B_p was first examined for all odd primes less than 61, since this is the maximum word length of BRLESC. The results were that B_p is prime for p = 3, 5, 7, 11, 13, 17, 19, 23, 31, 43. For p = 29, 37, 41, 47, 53, 59, B_p is composite with factors 59, 1777, 83, 283, 107, 2833 respectively.

B_{61} was tested by determining whether or not the congruence $2^{61} \equiv -1 \pmod{122k + 1}$ held for some k. For $k \leqq 51,365$ this congruence was not satisfied; and hence, if B_{61} has a factor, it must be between 6,266,531 and $\sqrt{(2^{61} + 1)/3}$.

Similarly, B_{67} was tested and found to have no factors less than or equal to 4,365,319 (k = 32,577). Time did not permit these to be extended further.

When the program became too time consuming, a new program was written to determine the set of B_p's that were not prime. The following method was used. A prime number q greater than three was generated. Then the smallest integer $n > 0$ was found such that $2^n \equiv 1 \pmod q$ or $2^n \equiv -1 \pmod q$. If $2^n \equiv 1 \pmod q$, then $2^{n+1} \equiv 2 \pmod q$ and the system of residues is cyclic with order n. Therefore, $2^n \not\equiv -1 \pmod q$ for all n, so that q is a factor of B_p for no p. Also, if $2^n \equiv -1 \pmod q$ and n is not a prime, then we can conclude that q is a factor of B_p for no p. To see this, assume there does exist some prime integer m such that $m > n$ and $2^m \equiv -1 \pmod q$. Since $2^n \equiv -1 \pmod q$ implies $2^{2n} \equiv 1 \pmod q$, we know by the above argument the system of residues is cyclic with order 2n. Therefore, $n < m < 2n$. By the algebra of congruences, $2^m - 2^n \equiv [(-1) - (-1)] \pmod q$ or $2^m - 2^n \equiv 0 \pmod q$. Since $2^m - 2^n = 2^n(2^{m-n} - 1)$ and q divides $(2^m - 2^n)$ but not 2^n, it follows that q divides $2^{m-n} - 1$. But this implies $2^{m-n} \equiv 1 \pmod q$. Since $m - n < n$, this result contradicts the assertion that n is the least integer such that $2^n \equiv \pm 1 \pmod q$. Hence, q is a factor of B_p for no p. Finally, when $2^n \equiv -1 \pmod q$ and n is prime, we have that q is a factor of $2^n + 1$. Since $q > 3$, q is, therefore, a factor of B_n.

This program has the advantage that, given a prime q, one can readily find the p such that q divides B_p, if such a p exists. Hence, a systematic check with each prime q will discover all p such that B_p has a factor in the group of integers with prime factors less than or equal to q.

It took BRLESC almost 22 hours to compute all primes q, $q \leq 299{,}087$, find an n such that $2^n \equiv 1$ or $-1 \pmod q$ and then determine whether or not n was prime. Of the 25,959 prime numbers less than or equal to 299,087, we found 1330 B_p's that were composite. Of these, 1262 B_p's had only one factor less than 299,087; 59 B_p's had two factors less than 299,087; 7 had three factors less than 299,087; and 2 had four factors less than 299,087. In examining 25,959 prime numbers, 5.4% turned out to be factors of the B_p's.

Finally, on the basis of these results, it would seem that prime B_p are more frequent than prime M_p. From the first 16 odd primes, there are 7 prime M_p compared with 10 prime B_p.

Below is a complete table giving all p such that B_p has a factor q, $q \leq 299{,}087$. Printed beside the p is the corresponding k such that $q = 2kp + 1$ is a factor of B_p.

LYNN S. MOHLER

NUMERICAL RESULTS

p	k	p	k	p	k	p	k
29	1	419	7	977	4	1613	12
37	24	421	5	1013	1	1621	9
41	1	443	55	1021	5,9	1669	14
47	3	449	217	1039	75	1699	35
53	1	461	108,120	1049	1	1733	1,40
59	24,315	479	4,40	1103	103	1789	12
73	12	499	164	1151	4,115	1823	3,12
83	3,7,16,936	509	1	1153	12	1889	1
89	1	541	80	1171	11,36	1901	1
97	5,8,164	557	4,112	1181	21,25	1933	72
107	3	569	9	1229	1	1973	1
113	1,216	571	8	1237	8	1987	3
131	4	577	65	1249	17	2027	3
137	4,57	593	1	1283	3	2069	1,7
149	4	607	95	1289	1,9,12	2081	4
157	48	617	4	1291	11	2129	1,4
173	1,12	641	1,25,109	1307	4	2141	1
181	5	653	1	1327	3	2203	3
211	11	659	51,216	1361	4	2221	9
227	655	661	156	1399	12	2239	24
233	1,60	719	24	1409	1	2251	8
241	5	727	8	1439	7	2273	1
251	475	743	15	1451	3	2281	5,21
263	3,175	751	183	1481	1,49	2339	4
271	3	761	1	1499	15	2341	21,48
281	1	769	24	1511	3	2347	3
283	3,111	809	1,9,12	1523	7	2377	29
293	1,45,57	821	4	1531	3	2381	48
311	103	877	17	1559	4	2383	12
331	8	881	13,33,40,85	1567	3	2393	1
337	32	883	12,167	1571	4	2399	7
367	3,27	887	3	1579	11	2447	3,4
373	81	947	4,7	1601	1	2477	9,13,24
397	17	953	1	1609	5	2549	1

p	k	p	k	p	k	p	k
2551	3	3583	3	4643	7	5867	7
2609	4	3593	1	4657	32	5927	15
2689	5	3631	3	4663	8	5939	4,12
2693	1,13	3643	12	4679	12,27	6011	3
2707	8	3671	3	4703	3	6053	1
2711	3,36	3677	13	4729	12	6079	12
2719	32	3691	3	4733	1	6101	1
2741	1,9	3761	1,4	4783	11	6113	1
2753	1	3769	5	4793	1	6163	3
2767	8	3821	1	4813	5	6173	1
2851	3	3881	9	4817	13	6199	11
2903	3	3917	4	4889	4	6269	4,10
2927	4	3947	7	4967	3	6329	1
2939	16	3967	35	4957	20	6337	17
2957	12	3989	37	5011	23	6367	8
2969	1	4001	4,28	5021	25	6449	1
2999	4	4013	28	5081	1,24	6521	1,16
3037	8	4049	9,12	5113	5,20	6569	4
3061	45	4051	8,11	5147	4	6571	8
3121	9,29	4073	1	5189	25	6581	1
3203	7	4139	7	5309	4	6653	12
3209	4	4201	8	5333	1	6689	21
3221	21	4229	9	5381	4	6691	8,15
3253	20,36	4259	12	5399	15	6709	12
3307	3,23	4327	20	5437	5	6739	4,9
3323	7	4349	1,9	5441	1	6761	1
3329	1	4357	20	5501	1	6793	5
3361	8	4373	1	5569	12	6803	3
3389	1	4391	3,15	5647	8	6823	11
3391	3	4409	1	5669	9	6863	3
3413	1	4421	9	5741	1	6871	8
3449	1	4441	9	5783	7	6883	20
3457	8	4481	1	5813	21	6911	3
3491	3	4513	17	5827	23	6947	7
3533	12	4517	4	5843	3	6961	9
3547	3	4547	3	5849	1	6991	3

p	k	p	k	p	k	p	k
7121	1	8447	12	10589	1	12251	4
7193	1	8513	1	10607	4	12289	5
7219	15	8663	7	10613	1	12301	8
7229	12	8677	5	10709	1	12329	1
7253	13	8693	1	10733	1	12377	4
7333	12	8741	1	10771	3	12487	3
7349	1	8753	16	10781	1	12541	8
7433	1	8779	11	10861	8	12577	8
7541	1	8783	7	10889	9	12601	9
7561	9,8	8969	1	10903	3	12637	9
7573	8	9029	1	10937	12	12653	1
7607	15	9091	3	11159	4	12689	4
7649	1	9221	1	11257	5	12763	3
7703	16,3	9293	1	11273	13	12791	4
7757	4	9419	4	11287	3	12809	9
7841	1	9473	1	11317	5	12821	1
7853	16	9479	4	11321	1	12911	1
7901	1	9587	15	11369	1	12933	12
7963	3	9629	1	11393	1	12983	3
8059	15	9677	4	11437	5	13001	1
8069	1	9689	1	11549	1	13037	4
8087	3	9769	12	11593	5	13049	1
8093	16,1	9923	7	11621	9	13163	3
8101	9	9931	15	11657	4	13183	8
8123	7	10061	1	11743	3	13229	1
8167	3	10243	11	11801	1	13297	5
8179	11	10253	1	11813	1	13313	1
8237	13	10259	4	11821	5	13331	4
8243	3	10271	3	11909	1,4	13381	5
8263	11	10303	3	11953	8	13417	5
8273	1	10313	1	12007	3	13553	1
8291	3	10357	12	12041	1	13591	3,8
8297	13,4	10391	3	12101	1	13649	1
8363	12	10427	4,3	12197	4	13669	5
8431	3	10529	1	12227	3	13721	9

p	k	p	k	p	k	p	k
13841	4	15401	1	17351	3	19709	1
13873	5	15569	1	17387	3	19739	7
13901	1	15629	1	17449	5	19889	1
13913	1	15647	7	17467	3	19913	1
14009	1	15737	4	17471	3	19919	7
14051	3	15767	3	17491	3	19979	4
14081	1	15773	1	17657	4	20011	3
14153	1	15907	3	17669	1,4	20021	4
14207	3,4,7	15923	3	17681	1	20063	7
14249	1	15937	8	17707	3	20147	7
14281	5	16001	1	17783	3	20249	1
14321	1	16061	9	17827	3	20369	1
14327	4	16127	3	17971	3	20393	1
14423	3	16139	4	17981	1	20441	1
14431	3	16253	1	18041	1	20641	5
14461	5	16301	1	18149	1	20693	1
14489	1	16381	5	18191	3	20743	3
14561	1	16411	3	18233	1	20753	1
14621	1	16421	1	18251	4	20789	1
14657	9	16493	1	18341	1	20807	4
14669	1	16553	1	18461	1	20921	1
14723	3	16573	8	18523	8	21011	3
14741	1	16607	3	18773	1	21013	5
14747	4	16619	4	18911	3	21089	1
14771	4	16673	1	18959	4	21149	1
14869	5	16747	3	19139	4	21179	7
15061	5	16763	7	19183	3	21221	1
15101	1	16931	4	19259	4	21227	3
15107	7	17107	3	19301	1	21341	1
15131	3	17159	4	19373	1	21391	3
15161	1	17183	3	19433	1	21487	3
15173	1	17207	7	19553	1	21563	3
15233	1	17231	3	19597	5	21647	4
15269	1	17321	4	19603	3	21701	1
15391	3	17333	1	19661	1	21713	1

p	k	p	k	p	k	p	k
21727	3	23753	1	26189	1	29201	1
21737	4	23831	4	26371	3	29411	3
21893	1	23833	5	26407	3	29453	1
21929	4	23909	1	26501	1	29483	3
21997	5	23911	3	26573	1	29663	3
22003	3	23981	1	26597	4	29873	1
22013	1	24023	3	26633	1	30011	4
22067	3,4	24071	3	26641	5	30187	3
22111	3	24281	1	26729	4	30269	1
22123	3	24469	5	26821	5	30341	4
22133	1	24473	1	26849	1	30389	1
22189	5	24509	1	26927	4	30431	3
22273	5	24527	3	26947	3	30449	1
22343	3	24623	3	26993	1	30467	3
22349	1,4	24631	3	27077	4	30539	4
22409	1	24659	4	27143	3	30677	4
22433	1	24671	4	27197	4	30689	1
22447	3	24691	3	27281	1	30773	1
22469	1	24749	1	27527	4	30911	3
22481	1	24971	3	27581	1	30971	4
22541	1	25073	1	27691	3	31063	3
22787	4	25147	3	27773	1	31181	4
22811	4	25229	1	27809	1	31223	3
22853	1	25247	3	27851	3	31253	1
22861	5	25367	3	27893	1	31327	3
23081	4	25457	4	27947	4	31469	1
23321	1,4	25537	5	27983	3	31649	1
23417	4	25583	3	28001	1	31721	1
23531	4	25601	1	28087	3	31723	3
23561	1	25673	1	28793	1	31793	1
23567	3	25763	3	28901	1	31883	3
23603	3	25841	1	28949	1	32009	1
23669	1	25867	3	28961	1	32141	1
23677	5	25913	1	29021	1	32323	3
23741	4	25951	3	29033	1	32363	3

p	k	p	k	p	k	p	k
32381	1	35081	1	38371	3	42089	1
32443	3	35201	4	38453	1	42221	1
32561	1,4	35327	4	38501	1	42331	3
32573	1	35573	1	38669	1	42473	1
32633	1	35591	4	38783	3	42643	3
32789	1,4	35759	4	38861	1	42703	3
32933	1	35831	3	38873	1	42727	3
32939	4	35863	3	38933	1	42821	1
32957	4	35933	1	39089	1	43013	1
33053	1	35993	1	39163	3	43313	1
33247	3	36263	3	39233	1	43403	3
33329	4	36353	1	39443	3	43411	3
33461	1	36629	1	39511	3	43541	1
33521	1	36691	3	39521	1	43649	1
33569	1	36761	1	39563	3	43661	1
33617	4	36791	3	39569	1	43721	1
33713	1	36821	1	39791	3	43793	1
33749	1	36929	1	39953	1	44129	1
33773	1	36931	3	39989	1	44189	1
33791	3	36943	3	40123	3	44249	1
33809	1	37013	1	40127	3	44263	3
33941	1	37049	1	40193	1	44273	1
34211	3	37139	4	40343	3	44483	3
34253	1	37181	1	40853	1	44501	1
34267	3	37253	1	40949	1	44623	3
34327	3	37307	3	41081	1	44729	1
34367	3	37447	3	41381	1	44909	1
34487	3	37643	3	41609	1	44987	3
34603	3	37747	3	41621	1	45053	1
34871	3	37853	1	41669	1	45329	1
34913	1	38189	1	41729	1	45569	1
34949	1	38201	1	41887	3	45641	1
35023	3	38327	3	41911	3	45887	3
35051	4	38333	1	41969	1	45971	3
35069	1	38351	3	42023	3	46181	1

p	k	p	k	p	k	p	k
46229	1	52121	1	57773	1	64901	1
46349	1	52289	1	57881	1	65129	1
46589	1	52361	1	58013	1	65309	1
46703	3	52553	1	58049	1	65393	1
46723	3	52733	1	58193	1	65633	1
46751	3	53093	1	58601	1	66029	1
47051	3	53309	1	58889	1	66173	1
47189	1	53453	1	59021	1	66593	1
47501	1	53549	1	59369	1	66701	1
47513	1	53849	1	59393	1	66749	1
47609	1	54101	1	59453	1	67121	1
47741	1	54293	1	59513	1	67169	1
47743	3	54401	1	59621	1	67181	1
48029	1	54413	1	59981	1	67349	1
48221	1	54773	1	60149	1	67433	1
48413	1	54941	1	60293	1	67733	1
48593	1	55229	1	60449	1	68261	1
48761	1	55469	1	60509	1	68489	1
49193	1	55661	1	60689	1	68669	1
49253	1	55673	1	60761	1	69029	1
49391	3	55721	1	60773	1	69341	1
49433	1	55733	1	61409	1	69593	1
49481	1	55829	1	61469	1	69809	1
49747	3	55889	1	61961	1	69941	1
49853	1	56009	1	62213	1	70061	1
50021	1	56081	1	62501	1	70181	1
50261	1	56393	1	62753	1	70313	1
50273	1	56489	1	62981	1	70589	1
50513	1	56681	1	63113	1	70769	1
50741	1	56909	1	63929	1	70793	1
50873	1	56921	1	64301	1	70853	1
50969	1	57041	1	64373	1	70901	1
50993	1	57149	1	64709	1	71453	1
51521	1	57329	1	64793	1	71693	1
51893	1	57413	1	64853	1	71741	1

p	k	p	k	p	k	p	k
71849	1	78653	1	84713	1	93113	1
72101	1	78713	1	84761	1	93581	1
72161	1	79181	1	85049	1	93893	1
72269	1	79349	1	85061	1	93941	1
73421	1	79433	1	85121	1	94229	1
73553	1	79589	1	85133	1	94421	1
73589	1	79613	1	85313	1	95261	1
73613	1	79769	1	85601	1	95393	1
73673	1	79841	1	85733	1	95549	1
73709	1	79889	1	85829	1	95561	1
74201	1	80309	1	85853	1	95789	1
74381	1	80369	1	86441	1	95813	1
74729	1	80669	1	87149	1	95873	1
74933	1	80681	1	87221	1	96269	1
75041	1	81281	1	87701	1	96293	1
75149	1	81509	1	88661	1	96461	1
75161	1	81629	1	89153	1	96581	1
75329	1	81701	1	89909	1	96989	1
75353	1	81929	1	90089	1	97001	1
75389	1	82073	1	90173	1	97241	1
75689	1	82193	1	90281	1	97829	1
75821	1	82493	1	90641	1	98321	1
75833	1	82529	1	90749	1	98369	1
75941	1	82601	1	90833	1	98453	1
76001	1	82721	1	91121	1	98561	1
76421	1	82793	1	91193	1	98573	1
76781	1	82889	1	91373	1	98621	1
77261	1	83813	1	91433	1	98669	1
77513	1	83873	1	91529	1	98849	1
77813	1	84401	1	91841	1	98981	1
77847	1	84449	1	92681	1	99041	1
78173	1	84509	1	92849	1	99089	1
78233	1	84533	1	92861	1	99173	1
78341	1	84629	1	92993	1	99689	1
78509	1	84653	1	93053	1	99761	1

p	k	p	k	p	k	p	k
100361	1	108401	1	115781	1	125201	1
100493	1	108821	1	116969	1	125693	1
100913	1	108869	1	117041	1	125921	1
101333	1	108929	1	117101	1	126653	1
101429	1	109001	1	117269	1	126713	1
101681	1	109229	1	117329	1	127373	1
101693	1	109313	1	117989	1	127481	1
101789	1	109481	1	118169	1	127493	1
101921	1	109541	1	118361	1	127541	1
102149	1	109793	1	118589	1	127709	1
102293	1	109841	1	119429	1	127733	1
102461	1	110609	1	119513	1	127973	1
102593	1	111029	1	119849	1	128153	1
102653	1	111053	1	119921	1	128321	1
102881	1	111509	1	119981	1	128549	1
103349	1	111641	1	120293	1	128669	1
103409	1	111773	1	120833	1	128813	1
103613	1	111833	1	120941	1	128993	1
104033	1	112181	1	121853	1	129221	1
104369	1	112289	1	122021	1	129281	1
104393	1	112349	1	122201	1	129401	1
104561	1	113153	1	122273	1	129509	1
104729	1	113189	1	122393	1	129581	1
104789	1	113213	1	122861	1	129749	1
105173	1	113453	1	123269	1	129953	1
105401	1	113513	1	123341	1	130241	1
105533	1	114221	1	123401	1	131321	1
105701	1	114269	1	123449	1	131441	1
105929	1	114641	1	124121	1	131861	1
106121	1	114749	1	124133	1	131909	1
106433	1	114773	1	124433	1	131933	1
107021	1	115001	1	124493	1	132329	1
107441	1	115061	1	124529	1	132701	1
107741	1	115469	1	124769	1	132893	1
108089	1	115553	1	124781	1	133013	1

p	k	p	k
133649	1	140069	1
133709	1	140249	1
133949	1	140681	1
134489	1	140813	1
134609	1	141353	1
134789	1	141413	1
135029	1	142193	1
135221	1	142589	1
135281	1	143249	1
135329	1	143501	1
135449	1	143609	1
135461	1	143873	1
135533	1	144341	1
135581	1	144569	1
135893	1	145109	1
136133	1	145121	1
136541	1	145709	1
136949	1	145721	1
137201	1	145949	1
137369	1	146141	1
137393	1	146213	1
137573	1	146669	1
137849	1	146801	1
137993	1	147029	1
138041	1	147089	1
138389	1	147401	1
138581	1	147629	1
138629	1	148013	1
138821	1	148829	1
138893	1	148853	1
139109	1	149021	1
139313	1	149153	1
139409	1	149213	1
139589	1	149333	1
139721	1	149843	1

REFERENCES

[1] Lehmer, D. H. An Extended Theory of Lucas' Function. Annals of Mathematics, Vol. 31 (1930), pp. 419-448.

[2] Ore, Oystein. Number Theory and its History. McGraw-Hill Book Company, Inc., New York, (1948).

[3] Selfridge, J. I. and Hurwitz, Alexander. Fermat Numbers and Mersenne Numbers. Mathematics of Computation, Vol. XVIII, No. 85 (1964).

[4] Uspensky, J. V. and Heaslet, M. A. Elementary Number Theory. McGraw-Hill Book Company, Inc., New York (1939).

DISTRIBUTION LIST

No. of Copies	Organization
20	Commander Defense Documentation Center ATTN: TIPCR Cameron Station Alexandria, Virginia 22314
1	Director Institute for Defense Analyses 400 Army-Navy Drive Arlington, Virginia 22202
1	Commanding General U. S. Army Materiel Command ATTN: AMCRD-RP-B Washington, D. C. 20315
1	Commanding General U. S. Army Engineer Research & Development Laboratories ATTN: STINFO Branch Fort Belvoir, Virginia 22060
1	Commanding Officer U. S. Army Combat Developments Command Artillery Agency Fort Sill, Oklahoma 73503
2	Commanding Officer U. S. Army Research Office (Durham) ATTN: CRD-AA-IPL, Case 1045 (1 cy) Box CM, Duke Station Durham, North Carolina 27706
3	Chief, Bureau of Naval Weapons ATTN: DLI-3 Department of the Navy Washington, D. C. 20360

No. of Copies	Organization
1	Commander U. S. Naval Ordnance Laboratory White Oak Silver Spring, Maryland 20910
1	Superintendent U. S. Naval Observatory Washington, D. C. 20390
1	Superintendent U. S. Naval Postgraduate School ATTN: Technical Reports Section Monterey, California 93940
1	Chief of Naval Research Department of the Navy Washington, D. C. 20360
1	Director National Bureau of Standards Connecticut Ave. & Van Ness St., N.W. Washington, D. C. 20234
1	TRW Space Technology Laboratories ATTN: D. D. Carpenter One Space Park Redondo Beach, California 90277
1	University of Wisconsin ATTN: U. S. Army Mathematics Research Center Madison, Wisconsin 53706

Aberdeen Proving Ground

Ch, Tech Lib

Air Force Ln Ofc
Marine Corps Ln Ofc
Navy Ln Ofc
CDC Ln Ofc

Unclassified

Security Classification

DOCUMENT CONTROL DATA - R&D

(Security classification of title, body of abstract and indexing annotation must be entered when the overall report is classified)

1. ORIGINATING ACTIVITY *(Corporate author)* U.S. Army Ballistic Research Laboratories Aberdeen Proving Ground, Maryland	2a. REPORT SECURITY CLASSIFICATION Unclassified 2b. GROUP

3. REPORT TITLE

PRIMALITY OF A CERTAIN CLASS OF INTEGERS

4. DESCRIPTIVE NOTES *(Type of report and inclusive dates)*

5. AUTHOR(S) *(Last name, first name, initial)*

Mohler, Lynn S.

6. REPORT DATE August 1965	7a. TOTAL NO. OF PAGES 21	7b. NO. OF REFS 4

8a. CONTRACT OR GRANT NO.	9a. ORIGINATOR'S REPORT NUMBER(S) Report No. 1300
b. PROJECT NO. 1P014501A14B	
c.	9b. OTHER REPORT NO(S) *(Any other numbers that may be assigned this report)*
d.	

10. AVAILABILITY/LIMITATION NOTICES

Qualified requesters may obtain copies of this report from DDC.

11. SUPPLEMENTARY NOTES	12. SPONSORING MILITARY ACTIVITY U.S. Army Materiel Command Washington, D. C.

13. ABSTRACT

This report is concerned with determining the primeness of the members of a class of numbers of the form, $B_p = \frac{2^p + 1}{3}$, where p is an odd prime. This class is similar to the Mersenne and Fermat numbers. A theorem is proven which characterizes the factors of B_p. This study was conducted using BRLESC, the high-speed digital computer at BRL and a description is given of the program used. Finally, the B_p's that were found to be prime as well as the B_p's that were found to be composite are tabulated.

DD FORM 1 JAN 64 1473

Unclassified

Security Classification

Unclassified
Security Classification

14. KEY WORDS	LINK A ROLE	LINK A WT	LINK B ROLE	LINK B WT	LINK C ROLE	LINK C WT
Primality Related to Fermat and Mersenne primes						

INSTRUCTIONS

1. ORIGINATING ACTIVITY: Enter the name and address of the contractor, subcontractor, grantee, Department of Defense activity or other organization *(corporate author)* issuing the report.

2*a*. REPORT SECURITY CLASSIFICATION: Enter the overall security classification of the report. Indicate whether "Restricted Data" is included. Marking is to be in accordance with appropriate security regulations.

2*b*. GROUP: Automatic downgrading is specified in DoD Directive 5200.10 and Armed Forces Industrial Manual. Enter the group number. Also, when applicable, show that optional markings have been used for Group 3 and Group 4 as authorized.

3. REPORT TITLE: Enter the complete report title in all capital letters. Titles in all cases should be unclassified. If a meaningful title cannot be selected without classification, show title classification in all capitals in parenthesis immediately following the title.

4. DESCRIPTIVE NOTES: If appropriate, enter the type of report, e.g., interim, progress, summary, annual, or final. Give the inclusive dates when a specific reporting period is covered.

5. AUTHOR(S): Enter the name(s) of author(s) as shown on or in the report. Enter last name, first name, middle initial. If military, show rank and branch of service. The name of the principal author is an absolute minimum requirement.

6. REPORT DATE: Enter the date of the report as day, month, year; or month, year. If more than one date appears on the report, use date of publication.

7*a*. TOTAL NUMBER OF PAGES: The total page count should follow normal pagination procedures, i.e., enter the number of pages containing information.

7*b*. NUMBER OF REFERENCES: Enter the total number of references cited in the report.

8*a*. CONTRACT OR GRANT NUMBER: If appropriate, enter the applicable number of the contract or grant under which the report was written.

8*b*, 8*c*, & 8*d*. PROJECT NUMBER: Enter the appropriate military department identification, such as project number, subproject number, system numbers, task number, etc.

9*a*. ORIGINATOR'S REPORT NUMBER(S): Enter the official report number by which the document will be identified and controlled by the originating activity. This number must be unique to this report.

9*b*. OTHER REPORT NUMBER(S): If the report has been assigned any other report numbers *(either by the originator or by the sponsor)*, also enter this number(s).

10. AVAILABILITY/LIMITATION NOTICES: Enter any limitations on further dissemination of the report, other than those imposed by security classification, using standard statements such as:

(1) "Qualified requesters may obtain copies of this report from DDC."

(2) "Foreign announcement and dissemination of this report by DDC is not authorized."

(3) "U. S. Government agencies may obtain copies of this report directly from DDC. Other qualified DDC users shall request through ________________."

(4) "U. S. military agencies may obtain copies of this report directly from DDC. Other qualified users shall request through ________________."

(5) "All distribution of this report is controlled. Qualified DDC users shall request through ________________."

If the report has been furnished to the Office of Technical Services, Department of Commerce, for sale to the public, indicate this fact and enter the price, if known.

11. SUPPLEMENTARY NOTES: Use for additional explanatory notes.

12. SPONSORING MILITARY ACTIVITY: Enter the name of the departmental project office or laboratory sponsoring *(paying for)* the research and development. Include address.

13. ABSTRACT: Enter an abstract giving a brief and factual summary of the document indicative of the report, even though it may also appear elsewhere in the body of the technical report. If additional space is required, a continuation sheet shall be attached.

It is highly desirable that the abstract of classified reports be unclassified. Each paragraph of the abstract shall end with an indication of the military security classification of the information in the paragraph, represented as *(TS)*, *(S)*, *(C)*, or *(U)*.

There is no limitation on the length of the abstract. However, the suggested length is from 150 to 225 words.

14. KEY WORDS: Key words are technically meaningful terms or short phrases that characterize a report and may be used as index entries for cataloging the report. Key words must be selected so that no security classification is required. Idenfiers, such as equipment model designation, trade name, military project code name, geographic location, may be used as key words but will be followed by an indication of technical context. The assignment of links, rules, and weights is optional.

Unclassified
Security Classification