ON ALL OF MERSENNE'S NUMBERS PARTICULARLY M_{193}

BY H. S. UHLER

YALE UNIVERSITY

Communicated by F. D. Murnaghan, January 15, 1948

On November 27, 1947, the author finished investigating, by application of the Lucasian sequence 4, 14, 194, 37634, $\cdots$, the factorizability of Mersenne's number $M_{193} = 2^{193} - 1 =$ 1255 42034 70773 36152 76715 78846 41533 28322 04710 88892 80690 25791. The 192nd residue had the value 542 45701 25193 90814 13211 43009 56802 04633 04970 79432 42801 51282 which, being non-zero, shows[1] that M_{193} is composite in character. A sufficiently detailed account of the procedure followed and of the underlying basic theorem may be found in the author's first paper[2] on Mersenne's numbers. Suffice it to record two facts. After the date given above the data of the entire set of original work-strips were checked for the third time with an auxiliary modulus in conformity with the condition $(M_{193}q_k + r_k + 2) \equiv r_{k-1}^2 (\text{mod } 10^7 + 1)$, where q and r denote "quotient" and "remainder," respectively. The approximation to the reciprocal of M_{193} used in the latest work had the value 0.(58 zeros) 79654 59555 66226 13851 44401 98883 85590 27955 52277 59630 93930 37006 37523 90143 41987 11093 10854 40700 94876 19334 41734 25085 25958 34273 96290 7$\cdots$. The check multiplication gave $(M_{193})(1/M_{193})_a = 1 + 1.98 \times 10^{-126}$.

With regard to the 55 numbers of the form $2^p - 1$ (where p is a prime not exceeding 257) considered by Mersenne, the following brief report on recent progress made in their study and the present state of our knowledge may be timely because of its definitive character. In the year 1935 there remained[3] six Mersenne numbers which had not been investigated with respect to their prime or composite properties. These corresponded to $p = 157, 167, 193, 199, 227$ and 229.

In leisure hours the present writer began the investigation of M_{157} in the spring of the year 1944 and finished the entire set with M_{193} on the date given above. These M_p's were taken up in random order in the vain hope of discovering a prime number greater than $2^{127} - 1$. More specifically the final residues for M_{157}, M_{167}, M_{229}, M_{199} and M_{227} were obtained, respectively, on Aug. 11, 1944, Dec. 2, 1944, Feb. 9, 1946, July 27, 1946, and June 4, 1947. (The manuscript on M_{227} was accepted for publication in the *Bulletin of the American Mathematical Society* on July 17, 1947.) Since all six M_p's were found to be composite the earlier status of Mersenne's remarks has not been changed but a lacuna in our knowledge has been filled. The next extremely difficult step will consist in the discovery of all of the as yet unknown factors of Mersenne's numbers.

Mersenne said[3] that the only values of p not greater than 257 which

make M_p prime are 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 and 257. Comparison of this list with the correct data recorded in the top line of the table presented below shows that Mersenne made five mistakes. $p = 67$ and 257 do not yield prime values for M_p, and $p = 61$, 89 and 107 were not included in his list of special primes.

With reference to explicit factoring, attention should be called to a valuable paper[4] by Professor D. H. Lehmer entitled "On the Factors of $2^n \pm 1$." His investigations on 76 numbers unveiled eleven factors which fall within Mersenne's range. Incidentally two of his new factors confirmed the present writer's final residues for M_{167} and M_{229}.

p	CHARACTER OF M_p
2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127	Prime
11, 23, 29, 37, 41, 43, 47, 53, 59, 67, 71, 73, 79, 113	Composite and fully factored
151, 163, 173, 179, 181, 223, 233, 239, 251	Two or more prime factors found
83, 97, 131, 167, 191, 197, 211, 229	Only one prime factor known
101, 103, 109, 137, 139, 149, 157, 193, 199, 227, 241, 257	Composite but no factor known

[1] Lehmer, D. H., *Jour. London Math. Soc.*, **9–10**, 162–165 (1934–1935).
[2] Uhler, H. S., *Proc. Nat. Acad. Sci.*, **30**, 314–316 (1944).
[3] Archibald, R. C., *Scripta Mathematica*, **3**, 112–119 (1935).
[4] Lehmer, D. H., *Bull. Amer. Math. Soc.*, **53**, 164–167 (1947).

NEW TYPES OF CONGRUENCES INVOLVING BERNOULLI NUMBERS AND FERMAT'S QUOTIENT

BY H. S. VANDIVER

DEPARTMENT OF APPLIED MATHEMATICS, UNIVERSITY OF TEXAS

Communicated January 17, 1948

In another paper[1] the writer gave the relation

$$(mb + k)^n = \sum_{a=1}^{r} \binom{r}{a} (-1)^{a-1} \frac{S_n(m, k, a)}{a}; \quad r > n; \qquad (1)$$

where we define the Bernoulli numbers b_n by means of the recursion formula $(b + 1)^n = b_n$; $n > 1$, the left-hand member being expanded in full and b_s substituted for b^s, and the left-hand member of (1) is interpreted in the same way;

$$S_n(m, k, a) = \sum_{i=0}^{a-1} (im + k)^n; \qquad 0^0 = 1,$$

m and k are any integers with $m \neq 0$. In the present paper we shall employ (1) as well as other known relations to obtain various congruences. The principal results proved seem to be (5), (6b), (7) and (20).