

condition  $\sum_{k=1}^n a_k = 0$ . But  $x_2 - x_1$  shows that this condition is not sufficient. Pólya remarked that if (25) has infinitely many solutions we can not have  $a_1 \geq 0$ ,  $a_1 + a_2 \geq 0$ ,  $\dots$ ,  $a_1 + a_2 + \dots + a_n \geq 0$ . The characterization of the forms which satisfy (26) seems a difficult problem.

Finally we mention two more questions:

(1) Can the inequalities  $p_{n+1} - p_n < p_{n+2} - p_{n+1} < \dots < p_{n+k} - p_{n+k-1}$  have infinitely many solutions for every fixed  $k$ ?

(2) Is it true that the number of solutions of  $p_{k+1} - p_k > p_k - p_{k-1}$ ,  $k \leq n$  is  $n/2 + o(n)$ ? As we already have stated we can show that the number of solutions in question is between  $c_1 n$  and  $(1 - c_1)n$ .

SYRACUSE UNIVERSITY AND  
UNIVERSITY OF BUDAPEST

---

### ON MERSENNE'S NUMBER $M_{227}$ AND COGNATE DATA

H. S. UHLER

When  $p$  equals one of the 55 primes 2, 3, 5,  $\dots$ , 257 then, strictly speaking,  $M_p = 2^p - 1$  is called a Mersenne number. To obtain a clear perspective of the history of this special subject the reader may consult the interesting accurate paper by R. C. Archibald.<sup>1</sup> Without any superior value of  $p$ , it has been shown by E. Lucas that the prime or composite character of a number of the form  $2^p - 1$  ( $p$  prime) may be investigated by employing the sequence 3, 7, 47, 2207,  $\dots$  when  $p$  is of the form  $4n - 1$ , and the sequence 4, 14, 194, 37634,  $\dots$  when  $p = 4n + 1$ . In both cases the law of formation of the terms is  $s_k = s_{k-1}^2 - 2$ . However, it is no longer necessary to use the  $4n - 1$  Lucasian series since D. H. Lehmer<sup>2</sup> stated and proved the following theorem: "*The number  $N = 2^n - 1$ , where  $n$  is an odd prime, is a prime if, and only if,  $N$  divides the  $(n - 1)$ st term of the series*

$$S_1 = 4, S_2 = 14, S_3 = 194, \dots, S_k, \dots,$$

where  $S_k = s_{k-1}^2 - 2$ ." This justifies the use by the present writer of the second progression although 227 falls in the  $4n - 1$  class.

Received by the editors July 7, 1947.

<sup>1</sup> R. C. Archibald, *Mersenne's numbers*, Scripta Mathematica vol. 3 (1935) pp. 112-119.

<sup>2</sup> D. H. Lehmer, *On Lucas's test for the primality of Mersenne's numbers*, J. London Math. Soc. vol. 9-10 (1934-1935) pp. 162-165.

On June 4th, 1947 the writer finished calculating the 226th remainder of the Lucasian sequence 4, 14, 194, . . . as applied to the 69-digit number  $2^{227}-1=2156\ 79573\ 33720\ 51183\ 57336\ 12069\ 61570\ 45389\ 09715\ 53803\ 24579\ 84882\ 88819\ 93727$ . The result was  $r_{226}=1071\ 24133\ 67508\ 18344\ 33653\ 76892\ 98433\ 16050\ 93930\ 31886\ 49512\ 37078\ 23311\ 35950$ . Since this residual is not zero and since the calculations were performed with extreme care it follows that  $M_{227}$  is composite.

During the entire course of the work each arithmetical operation was checked with the auxiliary moduli  $10^5+1$  and  $10^8+1$ . After the date given above all of the work-strips of the whole set were again examined and checked with the modulus  $10^6+1$ , with a different computing machine, and in conformity with the formula of succession  $r_{k-1}^2 = M_{227}q_k + r_k + 2$ .

In addition to the theoretical probability of error indicated by the product of the three independent moduli  $10^5+1$ ,  $10^6+1$  and  $10^8+1$ , the reliability of the writer's method and work has been subjected to an a posteriori acid test in each of two instances. In a letter dated September 12th, 1946, Professor Lehmer informed me that he had discovered<sup>3</sup> ("this July 4th weekend") the factor 2349023 for  $M_{167}$  and the factor 1504073 for  $M_{229}$ . He then wrote: "It might be interesting now to try to verify your . . . final residue in each of these tests by computing Lucas' series modulus 2349023 and 1504073 and then see if the results are the same as those obtained from casting these numbers out of your final remainders." This friendly suggestion was followed by me with the results that the two 166th residues were congruent to 2160517 (mod 2349023), and the two 228th remainders were identical with the value 465373. The heretofore intentionally unpublished value of  $r_{166}$  is 59077 89471 97183 05021 04043 18653 76339 69475 17591 49076.

As explained in an earlier paper<sup>4</sup> the essential figures of each of the terms above the 8th of the specified Lucasian sequence were multiplied in order by the reciprocal of the chief modulus,  $M_{227}$ , in preference to direct division by  $M_{227}$ . The approximation to this reciprocal was computed to be  $(1/M_{227})_a = 0.(68\ \text{zeros})\ 46365\ 07688\ 35927\ 67321\ 64669\ 07693\ 45493\ 91709\ 45597\ 34472\ 38753\ 06629\ 88236\ 46998\ 17232\ 30809\ 13430\ 64583\ 44938\ 95187\ 64723\ 82742\ 71\ \dots$ . These figures were derived at once from the writer's earlier trustworthy

<sup>3</sup> D. H. Lehmer, *On the factors of  $2^n \pm 1$* , Bull. Amer. Math. Soc. vol. 53 (1947) pp. 164-167.

<sup>4</sup> H. S. Uhler, *First proof that the Mersenne number  $M_{167}$  is composite*, Proc. Nat. Acad. Sci. U. S. A. vol. 30 (1944) pp. 314-316.

value of  $(1/M_{229})_a$  and the obvious relation  $M_{227}^{-1} = 4M_{229}^{-1} + 12M_{229}^{-2} + \dots$ . Because  $(1/M_{227})_a$  was to be used 218 times as multiplier, the value just given was verified twice by multiplication by the exact value of  $M_{227}$ , once using octad segregation of the digits and again with nonad grouping. It was proved that the last figure (1) recorded for  $(1/M_{227})_a$  is too small by about 0.04 unit.

For future investigations it may be appropriate to record in this place the value of the tenth term of the sequence 4, 14, 194,  $\dots$  as carefully computed by the author.  $s_{10} = s_9^2 - 2 = 687\ 29682\ 40664\ 42772\ 38837\ 48623\ 17475\ 30924\ 24715\ 41086\ 46671\ 75219\ 26185\ 83088\ 48740\ 57909\ 57964\ 73288\ 30691\ 02561\ 04343\ 67796\ 63935\ 59517\ 20423\ 57306\ 59491\ 63446\ 06074\ 56471\ 28680\ 78287\ 60805\ 52030\ 24658\ 35943\ 90175\ 80883\ 91097\ 86661\ 85875\ 71741\ 55410\ 84494\ 92650\ 04751\ 67381\ 16850\ 59273\ 78181\ 89975\ 38392\ 60609\ 45226\ 53652\ 74850\ 90187\ 98812\ 03714$ . This term has 293 digits and it would be applicable to all odd primes less than and inclusive of  $p=971$  in  $2^p - 1 = M_p$ . If the speed of present or future electronic computing machines should cause the operators to run out of problems it might be worth while to apply one of the machines to testing the character of  $M_{971}$  where  $M_{971} + 1 = 2^{971} = 199\ 58403\ 09534\ 71981\ 16563\ 72713\ 03683\ 85660\ 67451\ 26043\ 54575\ 41502\ 54724\ 24372\ 11891\ 86896\ 40657\ 84957\ 96549\ 26357\ 01089\ 34244\ 68441\ 92495\ 24397\ 24379\ 88393\ 59366\ 07391\ 71798\ 28483\ 14203\ 20005\ 67295\ 10856\ 76517\ 53772\ 14443\ 62987\ 18265\ 33567\ 44543\ 92399\ 33308\ 10455\ 12087\ 03888\ 88855\ 26844\ 80441\ 57507\ 12090\ 68757\ 56041\ 64235\ 84952\ 30344\ 00992\ 78848$ . The accuracy of this power of 2 may be inferred from the following quotation of a sentence in a very recent letter from Dr. John W. Wrench, Jr. "Your value of  $2^{971}$  has been collated with mine on several occasions in the past two days, and agreement is perfect."

The writer is now engaged in applying the sequence 4, 14, 194,  $\dots$  to the investigation of the sole remaining doubtful  $M_p$  within Mersenne's range of surmise ( $p < 263$ ), namely  $2^{193} - 1$ .

YALE UNIVERSITY