MERSENNE AND FERMAT NUMBERS

RAPHAEL M. ROBINSON

1. **Mersenne numbers.** The Mersenne numbers are of the form 2^n-1. As a result of the computation described below, it can now be stated that the first seventeen primes of this form correspond to the following values of n:

2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281.

The first seventeen even perfect numbers are therefore obtained by substituting these values of n in the expression $2^{n-1}(2^n-1)$. The first twelve of the Mersenne primes have been known since 1914; the twelfth, $2^{127}-1$, was indeed found by Lucas as early as 1876, and for the next seventy-five years was the largest known prime. More details on the history of the Mersenne numbers may be found in Archibald [1]; see also Kraitchik [4]. The next five Mersenne primes were found in 1952; they are at present the five largest known primes of any form. They were announced in Lehmer [7] and discussed by Uhler [13].

It is clear that 2^n-1 can be factored algebraically if n is composite; hence 2^n-1 cannot be prime unless n is prime. Fermat's theorem yields a factor of 2^n-1 only when $n+1$ is prime, and hence does not determine any additional cases in which 2^{n-1} is known to be composite. On the other hand, it follows from Euler's criterion that if $n\equiv 0, 3 \pmod 4$ and $2n+1$ is prime, then $2n+1$ is a factor of 2^n-1. Thus, in addition to cases in which n is composite, we see that 2^n-1 is composite when $2n+1$ is prime as well as n, provided that $n \equiv 3 \pmod 4$ and $n>3$. Aside from this, factors of 2^n-1 are known only in individual cases. If no factor is known, the best way to find out whether 2^n-1 is prime is to apply a test due essentially to Lucas, but stated in a simplified form by Lehmer [6, Theorem 5.4].

THEOREM. *Let* $S_1=4$, $S_{k+1}=S_k^2-2$. *Then, for* $n>2$, *the number* 2^n-1 *is prime if and only if* $S_{n-1}\equiv 0 \pmod{2^n-1}$.

Alternatively, we may start with $S_1=10$; or, if $n\equiv 3 \pmod 4$, we may also use $S_1=3$. Such a test was first applied by Lucas in 1876 to show that $2^{127}-1$ is prime. By 1947, all of the numbers 2^n-1 with $n\leqq 257$ had been tested; if there had been no errors in the computations, this would have completed the proof or disproof of the various

Received by the editors February 7, 1954.

cases of Mersenne's conjecture of 1644. In 1951, the first application of an electronic computer to testing Mersenne numbers for primeness was made by A. M. Turing at the University of Manchester; however, no new primes were found, and no remainders were saved for purposes of comparison.

In 1952, a program for testing Mersenne numbers for primeness on the SWAC (the National Bureau of Standards' Western Automatic Computer, at the Institute for Numerical Analysis in Los Angeles), planned and coded by the author, using Lucas's test, was carried out, with the cooperation of D. H. Lehmer and the staff of the I. N. A. My thanks are due especially to Emma Lehmer, who did various auxiliary computations, including checking some of the results obtained against earlier results. The program was first tried on the SWAC on January 30, and two new primes were found that day; three other primes were found on June 25, October 7, and October 9.

At that time, the total memory of the SWAC consisted of 256 words of 36 binary digits each, exclusive of the sign. For the Mersenne test, half of this memory was reserved for commands. Since successive squarings of numbers less than the modulus 2^n-1 are required, this modulus was restricted to 64 words, so that the condition $n<64\cdot 36=2304$ was imposed. The estimated running time for the program was $0.25n^3+125n^2$ microseconds, and the actual time was in fair agreement with this. Thus, roughly speaking, the testing time was a minute for the first and an hour for the last of the five new primes. Each minute of machine time is equivalent to more than a year's work for a person using a desk calculator.

The output of the SWAC for each n was the least non-negative residue of $S_{n-1} \pmod{2^n-1}$, written to the base 16. This was a long string of zeros if 2^n-1 was prime, and otherwise was an apparently random sequence of digits. Every value of $n<2304$, for which no factor of 2^n-1 was known, was run twice on the SWAC; in case of disagreement, a third run was made. No remainder was accepted as correct until it had been obtained twice, and indeed on different days. (Although the bulk of this work was done in 1952, the checking was not complete in all respects until late in 1953. The submission of this report was delayed for this reason.) It is of course out of the question to print the hundreds of remainders obtained, but they will remain on file at the Institute for Numerical Analysis. [*Added in proof.* On July 1, 1954, the I.N.A. became a part of the University of California at Los Angeles; it is now known as Numerical Analysis Research.]

We shall confine ourselves here to mentioning various results of

earlier computations which have been verified or contradicted. (In a few cases, earlier computers had used the test with $S_1=3$; in these cases, the same computation was also made on the SWAC.) The six results of Uhler [12], for $n=157, 167, 193, 199, 227, 229$, were all checked by him by converting the corresponding SWAC remainders to decimal form, and found to be correct. The rest of the checking was done by Emma Lehmer. The three results of D. H. Lehmer [5], for $n=139, 149, 257$, were all verified. (Although Lehmer's remainder for $n=139$ had not been published, it was available for checking.) The result of Powers [10] for $n=241$ was found to be correct; the remainders from his earlier computations, for $n=103, 109$, had not been published, and were not available for checking. On the other hand, the four remainders of Fauquembergue [3], for $n=101, 103, 109, 137$ were all found to be incorrect, as was the remainder of Barker [2] for $n=167$.

If 2^n-1 is prime, so that $S_{n-1}\equiv 0 \pmod{2^n-1}$, then S_{n-2} is a solution of the congruence $x^2\equiv 2 \pmod{2^n-1}$. Thus $S_{n-2}\equiv \pm 2^{(n+1)/2} \pmod{2^n-1}$. The calculation of the next to the last remainder S_{n-2} was undertaken for the various known Mersenne primes, both with $S_1=4$ and with $S_1=10$, with the following results for the sign in the above congruence:

	$n=3$	5	7	13	17	19	31	61	89	107	127	521	607	1279	2203	2281
$S_1=4$	+	+	−	+	−	−	+	+	−	−	+	−	−	−	+	−
$S_1=10$	−	−	−	+	+	+	+	+	+	+	+	+	−	−	−	+

We have carried the program of testing Mersenne numbers for primeness about as far as is practicable using present day computers. The smallest untested Mersenne number is $2^{2309}-1$, which does not appear to be a case of exceptional interest. A more interesting case is $2^{8191}-1$, which should be prime according to a conjecture that 2^n-1 is always prime when n is a Mersenne prime. This conjecture is true for the first four cases, corresponding to the exponents

$$3 = 2^2 - 1, \quad 7 = 2^3 - 1, \quad 31 = 2^5 - 1, \quad \text{and} \quad 127 = 2^7 - 1.$$

The fifth case corresponds to $n=8191=2^{13}-1$. The corresponding Mersenne number was actually tested in 1953 by D. J. Wheeler on the Illiac, at the University of Illinois, one hundred hours of machine time being required. The remainder obtained was not zero, indicating that the number is composite, and the conjecture therefore false. According to Dr. Wheeler, considerable confidence may be placed in this result, since the computation was carefully checked.

2. **Fermat numbers.** The Fermat numbers are of the form 2^n+1. The only new result obtained here was that $2^{1024}+1$ is composite, and hence that a regular polygon with this number of sides cannot be constructed with ruler and compass.

The number 2^n+1 can be factored algebraically unless n is a power of 2. Factors are known in a few other cases. If no factor is known, the following test may be used.

THEOREM. *If* $n>1$, *then* 2^n+1 *is prime if and only if* $3^{2^{n-1}} \equiv -1 \pmod{2^n+1}$.

The program set up for testing Mersenne numbers on the SWAC was modified to apply to Fermat numbers. The range for the exponent n was the same, but with $n=2^m$, this yields $m \leqq 11$. Now $2^{2^m}+1$ is prime for $m=0, 1, 2, 3, 4$, and factors were known for $m=5, 6, 9, 11$. The Fermat numbers corresponding to $m=7, 8$ had been proved composite by Morehead and Western [**8**; **9**], and the remainders which they gave were found to be correct. (The necessary conversion of the SWAC result to decimal form was done by Emma Lehmer.) In the one new case, $m=10$, the least positive residue of $3^{2^{1023}} \pmod{2^{1024}+1}$ was found to be

	8x	4z258xu89	uw71y6w35	9z1vyy4u5	498v2v7v7
55y9wy98v	6yx3yy0x4	00u07877w	2866316zu	85wy92558	3y201x7x0
04w1zv076	yu292wxx4	0502v7567	226047037	308u12z32	887vyxu4x
51w50169z	6815w50u1	0wy653448	v953xy0w6	8uv4492z2	v1u564ux9
494x25wv7	wux26uuvw	4w5x12730	622y6z435	5xy035xx2	8798y8098

to the base 16, using 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, u, v, w, x, y, z as digits. Thus $2^{2^{10}}+1$ is composite. This result was first obtained in February 1952. As an extra check in this case, the test was recoded by Emma Lehmer; the modified test was run in January 1953, and the above remainder was verified.

Later in 1953, Selfridge [**11**] showed that this Fermat number has the factor $11131 \cdot 2^{12}+1$, which confirms the above result, but in a sense renders it obsolete even before it is submitted for publication. Selfridge also found a factor of $2^{2^{16}}+1$. Previously known factors of Fermat numbers may be found in Kraitchik [**4**]. Factors of $2^{2^m}+1$ are now known for $m=5, 6, 9, 10, 11, 12, 15, 16, 18, 23, 36, 38, 73$.

The first Fermat number of unknown character is $2^{8192}+1$, corresponding to $m=13$. The difficulty of testing this number is about the same as for the Mersenne number $2^{8191}-1$. It would probably be considerably easier to find some additional factors of Fermat numbers by trial.

References

1. R. C. Archibald, *Mersenne's numbers*, Scripta Mathematica vol. 3 (1935) pp. 112–119.

2. C. B. Barker, *Proof that the Mersenne number M_{167} is composite*, Bull. Amer. Math. Soc. vol. 51 (1945) p. 389.

3. E. Fauquembergue, *Nombres de Mersenne*, Sphinx-Œdipe, vol. 9 (1914) pp. 103–105; vol. 15 (1920) pp. 17–18.

4. M. Kraitchik, *On the factorization of $2^n \pm 1$*, Scripta Mathematica vol. 18 (1952) pp. 39–52.

5. D. H. Lehmer, *Note on the Mersenne number $2^{139}-1$*, Bull. Amer. Math. Soc. vol. 32 (1926) p. 522; *Note on Mersenne numbers*, ibid. vol. 38 (1932) pp. 383–384.

6. ———, *An extended theory of Lucas' functions*, Ann. of Math. vol. 31 (1930) pp. 419–448.

7. ———, *Recent discoveries of large primes*, Mathematical Tables and Other Aids to Computation vol. 6 (1952) p. 61; *A new Mersenne prime*, ibid. p. 205; *Two new Mersenne primes*, ibid. vol. 7 (1953) p. 72.

8. J. C. Morehead, *Note on Fermat's numbers*, Bull. Amer. Math. Soc. vol. 11 (1905) pp. 543–545.

9. J. C. Morehead and A. E. Western, *Note on Fermat's numbers*, Bull. Amer. Math. Soc. vol. 16 (1909) pp. 1–6.

10. R. E. Powers, *Certain composite Mersenne's numbers*, Proc. London Math. Soc. (2) vol. 15 (1916) p. xxii; *Note on a Mersenne number*, Bull. Amer. Math. Soc. vol. 40 (1934) p. 883.

11. J. L. Selfridge, *Factors of Fermat numbers*, Mathematical Tables and Other Aids to Computation vol. 7 (1953) pp. 274–275.

12. H. S. Uhler, *First proof that the Mersenne number M_{157} is composite*, Proc. Nat. Acad. Sci. U.S.A. vol. 30 (1944) pp. 314–316; *On all of Mersenne's numbers particularly M_{193}*, ibid. vol. 34 (1948) pp. 102–103; *Note on the Mersenne numbers M_{157} and M_{167}*, Bull. Amer. Math. Soc. vol. 52 (1946) p. 178; *On Mersenne's number M_{199} and Lucas's sequences*, ibid. vol. 53 (1947) pp. 163–164; *On Mersenne's number M_{227} and cognate data*, ibid. vol. 54 (1948) p. 379; *A new result concerning a Mersenne number*, Mathematical Tables and Other Aids to Computation vol. 2 (1946) p. 94.

13. ———, *A brief history of the investigations on Mersenne's numbers and the latest immense primes*, Scripta Mathematica vol. 18 (1952) pp. 122–131; *On the 16th and 17th perfect numbers*, ibid. vol. 19 (1953) pp. 128–131.

University of California, Berkeley