The Department of Computer Sciences at Purdue University generously contributed time on its new computer installation for this project. My thanks go especially to the director, Dr. Conte.

Purdue University
West Lafayette, Indiana

1. L. E. DICKSON, "Proof of the ideal Waring theorem for exponents 7–180," *Amer. J. Math.*, v. 58, 1936, p. 521–529.
2. ———, "Solution of Waring's problem," *Amer. J. Math.*, v. 58, 1936, p. 530–535.
3. ———, "The Waring problem and its generalizations," *Bull. Amer. Math. Soc.*, v. 42. 1936, p. 833–842.
4. K. MAHLER, "On the fractional parts of the powers of a rational number (II)," *Mathematika*, v. 4, 1957, p. 122–124.
5. HANS-HEINRICH OSTMANN, *Additive Zahlentheorie, zweiter Teil*, Springer-Verlag, 1956, p. 81–82.
6. S. S. PILLAI, "On Waring's problem," *Indian J. Math.* n.s., v. 2, 1936, p. 16–44.
7. D. RIDOUT, "Rational approximations to algebraic numbers," *Mathematika*, v. 4, 1957, p. 125–131.

Fermat Numbers and Mersenne Numbers

By J. L. Selfridge and Alexander Hurwitz

An IBM 7090 computer program, and results of testing Mersenne numbers $M_p = 2^p - 1$ with p prime, $p < 5000$, have been described by Hurwitz [1]. This paper describes modifications made to his program, and further computational results. The main results are that the Fermat number F_{14} is composite and that $2^p - 1$ is composite if $5000 < p < 6000$.

The computer program, originally written with the idea of testing $2^n - 1$ for $n = M_{13}$, soon showed that the machine makes occasional errors. At least four machine errors occurred during runs on this number before two results agreed. Due partly to the immediate availability of standby time, the program was then launched in the region $3300 < p < 5000$.

When this work was nearly complete, the routine was modified to incorporate a check modulo $2^{35} - 1$ after each squaring and another after each reduction modulo $2^p - 1$. These checks enabled the routine to recover and proceed automatically after a machine error. A message was printed that a squaring (or reduction) error had occurred. In fact, this happened several times.

Another modification enabled the program to compute 3^{2^n} modulo the Fermat number $F_m = 2^{2^m} + 1$. When $n = 2^m - 1$ the residue was output, with a result congruent to -1 if and only if F_m is prime.

After testing the program using F_{10} (see Robinson [5]), we proceeded to test F_{14}. The computation was divided into 64 parts, and the results of the first 25 of these were checked against those of Paxson [3], who very kindly sent us copies of his intermediate residues. The rest of the computation was done twice, with complete agreement. We have also checked the final residue obtained by Paxson [3] in the testing of F_{13}. The result that F_{14} is composite was announced in [2].

Received August 12, 1963. The preparation of this paper was sponsored by the Office of Naval Research.

TABLE 1

m	n	$R \bmod 2^{36}$	$R \bmod 2^{36} - 1$	$R \bmod 2^{35} - 1$
7	127	035100542404	514165207640	053153335617
8	255	531023263263	407614543114	344141643032
13	8191	607301005536	611677367012	031455470517
14	16383	622476273512	016631677043	161031465216
17	20	176536764625	415751561367	155276133751

TABLE 2

p	R	p	R	p	R
5023	35472	5479	17227	5783	15446
5077	27063	5503	26142	5813	25753
5081	74607	5527	41614	5839	24031
5099	67662	5573	34740	5851	37460
5113	20010	5581	31446	5857	11252
5153	52273	5591	52563	5869	00764
5309	40357	5641	21342	5879	52670
5333	44244	5647	40775	5897	30763
5351	05171	5653	50244	5923	16616
5387	54357	5669	57031	5953	32461
5407	51133	5689	32731	5987	66731
5419	70701	5693	47014		
5443	51737	5701	33577		
5471	52563	5737	07151		
5477	33022	5749	47641		

In addition, as a debugging aid for those who wish to test F_{17}, we computed $3^{2^{20}}$ modulo F_{17}. The complete testing of F_{17} would take 128 full weeks of machine time on the IBM 7090. It seems much more economical to search for small factors of F_{17} than to perform this test.

The final residues in the testing of F_7, F_8, F_{13} and F_{14}, and the residue of $3^{2^{20}} \pmod{F_{17}}$, have been put on punched cards, together with check sums. A summary of these residues is given in Table 1, and copies of the cards are available for checking purposes. The seven intermediate residues of $3^{2^n} \pmod{F_{14}}$ where $n \equiv 0 \pmod{2048}$, and the complete values of 3^{1024} and 3^{65536} are also on cards in the same format. In Table 1 the residue of $3^{2^n} \pmod{F_m}$ is described by listing its 12 least significant octal digits, and its remainder in octal modulo $2^{36} - 1$ and modulo $2^{35} - 1$.

Early in 1962, again partly because of available standby time, the Mersenne program, modified to check modulo $2^{35} - 1$, was run for all $2^p - 1$ for which no factor was known, with $5000 < p < 6000$. No primes were found. As in Hurwitz [1], the five least significant octal digits of S_{p-1} are listed in Table 2.

The results for $p < 3300$, mentioned by Hurwitz [1], have all been checked against the corresponding SWAC [5] and BESK [4] results. Reruns confirmed four

7090 errors, four BESK errors (2957, 2969, 3049 and 3109), and an incorrect SWAC result for 1889. The SWAC (October 1962) confirmed the 7090 residue.

UCLA Computing Facility
University of California, Los Angeles

1. ALEXANDER HURWITZ, "New Mersenne primes," *Math. Comp.*, v. 16, 1962, p. 249–251.
2. A. HURWITZ & J. L. SELFRIDGE, "Fermat numbers and perfect numbers," *Notices Amer. Math. Soc.*, v. 8, 1961, p. 601, abstract 587–104.
3. G. A. PAXSON, "The compositeness of the thirteenth Fermat number," *Math. Comp.*, v. 15, 1961, p. 420.
4. HANS RIESEL, "Mersenne numbers," *MTAC*, v. 12, 1958, p. 207–213.
5. RAPHAEL M. ROBINSON, "Mersenne and Fermat numbers," *Proc. Amer. Math. Soc.*, v. 5, 1954, p. 842–846.

Lucas' Test for Mersenne Numbers, $6000 < p < 7000$

By Sidney Kravitz and Murray Berg

Alexander Hurwitz [1] reported that he had applied Lucas' test to investigate the primality of the Mersenne Numbers $M_p = 2^p - 1$, p a prime, $3300 < p < 5000$, and discovered that M_{4253} and M_{4423} are prime numbers. Hurwitz [2] further states† that he tested all prime exponents between 5000 and 6000, where the corresponding M_p was not known to have a factor, without discovering any new Mersenne Primes.

TABLE

p	R	p	R	p	R
6007	07707	6247	00472	6659	75241*
6037	21420	6257	36710	6661	27165
6043	21605	6269	57356	6679	13275
6047	37000	6299	71037*	6701	07636
6053	53471	6329	25136*	6709	05700
6073	41646	6337	21676*	6733	35544
6079	15712	6359	51351	6763	01753
6089	32615	6361	10027*	6779	74306*
6091	02043	6451	23476	6791	41143
6133	42630	6469	51252	6823	14573*
6151	63451	6547	06546	6833	26431
6211	71252	6571	67142	6857	63102
6217	07377	6577	45051*	6907	46461*
6221	24166	6581	74210*	6911	63345
6229	06517	6599	77554	6971	65345
				6991	50365

The authors have tested the Mersenne Numbers $6000 < p < 7000$ without finding any new primes. A list of the five least significant octal digits of the S_{p-1}th remainder from the Lucas test ($S_1 = 4$) is given in the Table. Where a prime is missing from the list it indicates that a factor of the corresponding Mersenne Number was found by Riesel [3, 4] or that an unpublished† factor was found by

Received February 6, 1963. Revised April 26, 1963.

† See pages 146, 87, and 93 of this issue of *Mathematics of Computation*.