The Ideal Waring Theorem For Exponents 401-200,000

By Rosemarie M. Stemmler

1. The Problem. The classical Waring problem is the determination of the least number $g(k)$, k a positive integer, such that every positive integer is the sum of $g(k)$ k^{th} powers of integers $\geqq 0$. If

$$3^k = 2^k q + r, \quad 0 < r < 2^k, \quad \text{that is,} \quad q = [(\tfrac{3}{2})^k],$$

and

$$I(k) = 2^k + q - 2$$

the so-called ideal Waring theorem states that $g(k) = I(k)$ for every integer $k \geqq 1$.

The known facts are that $g(k) = I(k)$ for $k \neq 4, \neq 5$ and $1 \leqq k \leqq 400$. The calculations reported here extend this result up to $k = 200{,}000$. The conclusions are based on the work of Dickson [2] and Pillai [6] who proved independently for $k > 6$ and $k > 7$, respectively, that $g(k) = I(k)$ provided $2^k \geqq q + r + 3$, and [5] it has been established since that the ideal Waring theorem holds if $2^k \geqq q + r$, $k \neq 4, \neq 5$. Dickson proved in addition that if $2^k < q + r$, $k \geqq 7$ and $f = [(\tfrac{4}{3})^k]$

$$g(k) = I(k) + f \quad \text{or} \quad I(k) + f - 1$$

according as $2^k = fq + f + q$ or $2^k < fq + f + q$. Pillai actually constructed a table of 2^k, q and r for exponents to 100 which showed $2^k \geqq q + r + 3$ for $4 \leqq k \leqq 100$, whereas the upper bound 400 for k is due to theoretical considerations of Dickson's [3].

Actually Mahler [4] has shown that $r > 2^k - q$ is possible for only a finite number of positive integers k if at all. Mahler's theorem, a special case of which he applies to the Waring problem, is based on a theorem by Ridout [7] on rational approximations of algebraic numbers. According to Ridout the constant involved is not determinable by his method. If and when this can be done it will be possible also to decide whether the calculations here have completed the proof of the Waring theorem (for exponents other than 4 and 5), or to which exponent they would have to be continued.

To get a measure of the probability of finding an exceptional case among exponents beyond 200,000, the fractional parts of $(\tfrac{3}{2})^k$ were tabulated within intervals of length $\tfrac{1}{8}$. The results in the Table below make it probable that the sequence $\tfrac{3}{2}$, $(\tfrac{3}{2})^2$, $(\tfrac{3}{2})^3$, $\cdots$ is equidistributed (mod 1), in spite of the fact that in that table the interval I_7, which contains the fractional parts $\geqq \tfrac{3}{4}$ and $< \tfrac{7}{8}$, tends to hold a slightly larger share than the other intervals. Judging from the table it seems highly unlikely that a counterexample to the theorem will be found.

2. The Computation. The calculation was done on an IBM 7090 computer. The values of $(\tfrac{3}{2})^k$ were obtained mainly by "logical" operations and were stored in consecutive locations, the sign bits being used as part of the binary representation

---

Received August 13, 1963.

TABLE

Distribution of the fractional parts of $(\frac{3}{2})^k$

The interval I_t *contains the fractional parts* $\geqq (t-1)/8$ *and* $< t/8$.

k	I_1	I_2	I_3	I_4	I_5	I_6	I_7	I_8
100	15	9	12	15	11	13	8	17
200	27	24	19	30	22	27	26	25
300	40	37	32	40	37	39	44	31
400	53	48	44	49	53	49	58	46
500	63	66	59	61	63	58	70	60
600	78	79	70	72	78	70	83	70
700	94	94	80	82	91	82	98	79
800	105	105	90	94	104	98	111	93
900	116	114	103	106	118	113	125	105
1,000	128	124	122	118	131	126	133	118
2,000	243	246	253	236	257	249	265	251
3,000	365	400	375	369	369	368	399	355
4,000	476	534	497	494	496	491	534	478
5,000	605	652	626	620	616	609	647	625
6,000	719	784	743	746	736	736	773	763
7,000	827	911	866	873	846	856	897	924
8,000	962	1,036	990	998	980	979	1,015	1,040
9,000	1,091	1,138	1,107	1,127	1,109	1,116	1,129	1,183
10,000	1,200	1,271	1,243	1,249	1,238	1,214	1,269	1,316
20,000	2,480	2,525	2,460	2,484	2,473	2,462	2,559	2,557
30,000	3,732	3,739	3,696	3,738	3,708	3,710	3,831	3,846
40,000	4,980	4,983	4,897	4,953	4,980	5,010	5,128	5,069
50,000	6,162	6,198	6,165	6,179	6,240	6,264	6,436	6,356
60,000	7,439	7,420	7,421	7,418	7,503	7,516	7,682	7,601
70,000	8,665	8,646	8,688	8,683	8,743	8,763	8,914	8,898
80,000	9,904	9,870	9,916	9,916	9,987	10,045	10,200	10,162
90,000	11,153	11,155	11,194	11,137	11,211	11,292	11,456	11,402
100,000	12,462	12,379	12,475	12,350	12,494	12,512	12,714	12,614
110,000	13,644	13,648	13,709	13,597	13,775	13,775	13,991	13,861
120,000	14,929	14,963	14,949	14,840	15,037	14,999	15,246	15,037
130,000	16,123	16,226	16,227	16,124	16,289	16,259	16,475	16,277
140,000	17,354	17,491	17,525	17,369	17,591	17,434	17,765	17,471
150,000	18,538	18,804	18,770	18,597	18,804	18,681	19,059	18,747
160,000	19,806	20,056	20,040	19,819	20,054	19,888	20,301	20,036
170,000	21,038	21,246	21,244	21,108	21,355	21,206	21,559	21,244
180,000	22,290	22,453	22,483	22,346	22,589	22,492	22,784	22,563
190,000	23,534	23,688	23,744	23,576	23,867	23,760	24,024	23,807
200,000	24,823	24,929	25,030	24,824	25,144	24,975	25,270	25,005

of the numbers. Only as many 36-bit words of $1 - q/2^k$ were formed as were needed to show $r/2^k \leqq 1 - q/2^k$. For $2 \leqq k \leqq 10{,}000$ that inequality was established, and thereafter provision was made to print $r/2^k$ if the first 12 octal digits of $r/2^k$ should all be octal 7's since an exceptional value would certainly have to be of that form. No such fractional part was found to $k = 200{,}000$. As a time-saving device those left-most digits of q which would not affect $r/2^k$ up to $k = 200{,}000$ were progressively eliminated from $k = 130{,}000$ on. The first 10,000 exponents required between 4 and 5 minutes computer time, and the last run from 190,000 to 200,000 used about $1\frac{1}{2}$ hours. The distribution of fractional parts was checked through $k = 20$, and the determination of the appropriate interval tested through several sets of consecutive exponents. To guard against machine errors the computation was repeated through $k = 40{,}000$, and for larger k the last two words of $(\frac{3}{2})^{a+b}$ were periodically matched with the product of the previously tested end digits of $(\frac{3}{2})^a$ and $(\frac{3}{2})^b$.

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.