MATHEMATICS OF COMPUTATION
VOLUME 64, NUMBER 209
JANUARY 1995, PAGES 393–395

NEW FACTORS OF FERMAT NUMBERS

GARY B. GOSTIN

ABSTRACT. Forty-six new factors of Fermat numbers are given, along with a summary of the search limits.

Over the past several years the investigation reported here has resulted in the discovery of 46 new factors of Fermat numbers, which are listed in Table 1 (next page). These factors establish the compositeness of 42 Fermat numbers whose character was previously unknown, with F_{15}, F_{25}, F_{27}, and F_{147} having been previously factored. There are currently 161 known prime factors of 132 different Fermat numbers (see [1] and its updates for a summary of other known factors).

The method of factoring used here is similar to that of Hallyburton and Brillhart [3]. To determine whether $d_k = k \cdot 2^n + 1$, k odd, divides any $F_m = 2^{2^m} + 1$, where $m \leq n - 2$, the congruences $2^{2^m} \equiv -1 \pmod{d_k}$ are tested as follows. Begin with the residue $r_i = 2^{32}$ for $i = 5$. Then compute $r_i = r_{i-1}^2 \pmod{d_k}$. This operation is repeated until some i is found with $r_i \equiv -1 \pmod{d_k}$ or until $i = n - 2$. For any r_i, if $r_i \equiv -1 \pmod{d_k}$, then d_k divides F_i.

This method was implemented in C and assembly language for the 4-processor Convex C240. The program takes advantage of Convex's ASAP (Automatic Self-Allocating Processors) mechanism to execute in parallel on all available processors. All important routines are fully vectorized, and most routines are also parallelized. The program first generates a block of the next one million d_k's to test, and then uses a sieve to eliminate those d_k which are divisible by small primes. The surviving d_k are then tested using the above congruence.

Multiprecision numbers are squared by making use of the equality $(a \cdot 2^n + b)^2 = a^2 \cdot (2^{2n} + 2^n) - (a - b)^2 \cdot 2^n + b^2 \cdot (2^n + 1)$. In this way, a number of length $2n$ bits can be squared by squaring three numbers of length n bits, plus several shifts and adds. By recursively using this technique, the squaring operation is performed in $O(n^{1.58})$ time. Full multiprecision division is also avoided using the technique described in [2].

For each n, all $d_k = k \cdot 2^n + 1$, k odd, were tested up to a limit $k < L_k$. These limits are shown in Table 2 (next page).

All numbers in Table 1 are prime, since $2^{2^m} \equiv -1 \pmod{d_k}$, and 2^m exceeds the square root of d_k in each case. This follows from the $n - 1$ primality test of Proth, Pocklington, Lehmer, et al. Two factors are of particular interest.

Received by the editor October 12, 1992 and, in revised form, March 7, 1994.
1991 *Mathematics Subject Classification*. Primary 11-04, 11A51, 11Y11.

TABLE 1. New factors $d_k = k \cdot 2^n + 1$ of F_m

m	k	n	m	k	n	m	k	n
15	17753925353	17	251	85801657	254	885	16578999	887
25	1522849979	27	256	36986355	258	906	57063	908
27	430816215	29	259	36654265	262	1069	137883	1073
37	1275438465	39	301	7183437	304	1082	82165	1084
61	54985063	66	338	27654487	342	1123	25835	1125
64	17853639	67	353	18908555	355	1225	79707	1231
72	76432329	74	375	733251	377	1229	29139	1233
107	1289179925	111	376	810373	378	1451	13143	1454
122	5234775	124	417	118086729	421	1849	98855	1851
142	8152599	145	431	5769285	434	3506	501	3508
146	37092477	148	468	27114089	471	4258	1435	4262
147	124567335	149	547	77377	550	6208	763	6210
164	1835601567	167	620	10084141	624	6390	303	6393
178	313047661	180	635	4258979	645	6909	6021	6912
184	117012935	187	723	554815	730			
232	70899775	236	851	497531	859			

TABLE 2. Search limits

n	L_k	n	L_k
12–215	2^{31}	960–1951	2^{20}
216–463	2^{27}	1952–3935	2^{16}
464–959	2^{25}	3936–7903	2^{13}

The factorization of F_{256} proves the compositeness of the next member of the sequence $2^{2^{2^{2^n}}} + 1$, for $n = 3$. The factor of F_{635} has a difference $n - m = 10$, which is tied for the largest for the known factors. Also, it should be noted that Harvey Dubner independently discovered the factors of F_{6208} and F_{6390}, just a few months after the author.

Finally, each factor d_k of F_m in Table 1 was also tested to determine whether d_k^2 also divides F_m, by determining if $r = F_m \pmod{d_k^2}$ equals zero. No square factors were found. These calculations were checked in each case by verifying that $r \pmod{d_k} = 0$.

ACKNOWLEDGMENTS

The author would like to thank the many system managers at Convex Computer Corporation's world headquarters for allowing access to their "unused cycles". Their assistance and patience was essential in making the work reported here possible. Also, a special thanks to Wilfrid Keller for his kind assistance and helpful suggestions during the preparation of this paper.

BIBLIOGRAPHY

1. John Brillhart, D. H. Lehmer, J. L. Selfridge, Bryant Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of* $b \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ *up to high powers*, 2nd ed., Contemp. Math., vol. 22, Amer. Math. Soc., Providence, RI, 1988.
2. Gary B. Gostin and Philip B. McLaughlin, Jr., *Six new factors of Fermat numbers*, Math. Comp. **38** (1982), 645–649.
3. John C. Hallyburton, Jr. and John Brillhart, *Two new factors of Fermat numbers*, Math. Comp. **29** (1975), 109–112..

CONVEX COMPUTER CORPORATION, 3000 WATERVIEW PARKWAY, RICHARDSON, TEXAS 75083
E-mail address: `gostin@convex.com`