

FACTORS OF GENERALIZED FERMAT NUMBERS

HARVEY DUBNER AND WILFRID KELLER

ABSTRACT. Generalized Fermat numbers have the form $F_{b,m} = b^{2^m} + 1$. Their odd prime factors are of the form $k \cdot 2^n + 1$, k odd, $n > m$. It is shown that each prime is a factor of some $F_{b,m}$ for approximately $1/k$ bases b , independent of n . Divisors of generalized Fermat numbers of base 6, base 10, and base 12 are tabulated. Three new factors of standard Fermat numbers are included.

1. INTRODUCTION

Generalized Fermat numbers (GFNs) are of the form

$$(1) \quad F_{b,m} = b^{2^m} + 1, \quad b \geq 2.$$

When b is even, they have many characteristics of the heavily studied standard Fermat numbers $F_m = F_{2,m}$. For example, they have no algebraic factors; they may be prime; it is easy to prove primality; for a fixed base b , they are pairwise relatively prime; all prime factors must be of the form

$$(2) \quad P(k, n) = k \cdot 2^n + 1, \quad k \text{ odd}, \quad n > m.$$

When b is odd, most of these properties are shared by the numbers $F_{b,m}/2$. In particular, all their prime factors are also of the form (2).

While investigating the generalized Fermat numbers, some interesting relationships concerning divisibility characteristics were observed and then proved. Each prime (2) is shown to be a factor of some $F_{b,m}$ for almost exactly $1/k$ of the bases b , independent of n . It appears that the probability of each prime dividing a standard Fermat number is also $1/k$.

Divisors of generalized Fermat numbers of base 6, base 10, and base 12 are tabulated. Three new factors of standard Fermat numbers were discovered.

2. DIVISIBILITY RESULTS

There are approximately 160 known prime factors of Fermat numbers. It was natural to see if these factors were also factors of any other generalized Fermat numbers. What became immediately evident was that many of these factors were also factors of a surprisingly large number of GFNs, that is, $P(k, n)$ divided some $F_{b,m}$ for many values of the base b . In fact, examining the data

Received by the editor August 23, 1993 and, in revised form, January 10, 1994.

1991 *Mathematics Subject Classification.* Primary 11A51; Secondary 11B99, 11-04.

©1995 American Mathematical Society
0025-5718/95 \$1.00 + \$.25 per page

TABLE 1. Divisibility frequency. Bases tested from 2 to 1000, $10 < n < 1000$

| $3 \cdot 2^n + 1$ | | Prime divisor $5 \cdot 2^n + 1$ | | $7 \cdot 2^n + 1$ | |
|-------------------|--------------------|------------------------------------|--------------------|-------------------|--------------------|
| n | number of bases | n | number of bases | n | number of bases |
| 12 | 320 | 13 | 190 | 14 | 180 |
| 18 | 319 | 15 | 196 | 20 | 135 |
| 30 | 337 | 25 | 195 | 26 | 147 |
| 36 | 340 | 39 | 192 | 50 | 133 |
| 41 | 340 | 55 | 212 | 52 | 130 |
| 66 | 331 | 75 | 204 | 92 | 157 |
| 189 | 335 | 85 | 208 | 120 | 134 |
| 201 | 326 | 127 | 232 | 174 | 136 |
| 209 | 328 | average = 203.6 | | 180 | 136 |
| 276 | 334 | $999/k = 199.8$ | | 190 | 129 |
| 353 | 333 | | | 290 | 148 |
| 408 | 364 | | | 320 | 175 |
| 438 | 336 | | | 390 | 135 |
| 534 | 332 | | | 432 | 149 |
| average = 333.9 | | | | 616 | 141 |
| $999/k = 333.0$ | | | | 830 | 148 |
| | | | | average = 144.6 | |
| | | | | $999/k = 142.7$ | |

led to the observation that, on average, every prime $P(k, n)$ is a factor for $1/k$ of all bases, independent of n .

This is illustrated in Table 1. For $k = 3, 5$, and 7 all the primes $P(k, n)$ for n from 10 to 1000 were tested to see how many GFNs they divided. All bases from 2 to 1000 were tested. In each case the average number of bases for which $P(k, n)$ is a factor is close to $1/k$ times the number of bases considered. Basically the same pattern occurred for all values of k and n that we tested. The theoretical reason for this is developed in the next section.

3. DIVISIBILITY THEORY

The following [4, pp. 129–130] is Euler's criterion for the solvability of

$$(3) \quad b^N \equiv c \pmod{M}.$$

If M is any modulus with a primitive root, and $(c, M) = 1$, then the congruence (3) has a solution if and only if

$$(4) \quad c^{\phi(M)/d} \equiv 1 \pmod{M}, \quad \text{where } d = (N, \phi(M)).$$

Furthermore, when a solution exists, there are exactly d different solutions modulo M .

Indeed, since the prime $P(k, n)$ has a primitive root, we can apply the above criterion for $N = 2^m$, $c = -1$, and $M = P(k, n)$. In this case $\phi(P(k, n)) = k \cdot 2^n$ and $d = (2^m, k \cdot 2^n) = 2^m$, so the condition (4) guaranteeing the existence of a solution of

$$(5) \quad b^{2^m} \equiv -1 \pmod{P}, \quad P = P(k, n)$$

becomes

$$(6) \quad (-1)^{k \cdot 2^{n-m}} \equiv 1 \pmod{P},$$

and this relation holds because $n > m$ is assumed. We thus conclude that there are $d = 2^m$ solutions with $b < P$ of (5) for each m . But (5) is the equivalent to saying that P divides $F_{b,m}$ for the base b in question (note that $b = 0$ and $b = 1$ can never occur).

As the same reasoning applies to every $m \geq 0$, and for a given b the numbers $F_{b,m}$ have no odd factors in common, the total number of different base- b GFNs divisible by P is

$$(7) \quad b_{\text{tot}} = \sum_{m=0}^{n-1} 2^m = 2^n - 1,$$

hence the proportion of bases $b < P$ which have a GFN divisible by P is

$$(8) \quad \frac{b_{\text{tot}}}{P} = \frac{1 - 1/2^n}{k + 1/2^n}.$$

This is almost exactly $1/k$ for reasonably large n , a condition which holds for almost all P of interest. In the particular case of $k = 1$, primes $P = P(1, n)$ are the Fermat primes, which actually divide numbers $F_{b,m}$ for $2^n - 1$ of all $2^n + 1$ different bases modulo P .

If a prime divides GFNs for $1/k$ of the bases, it is reasonable to assume that the probability of dividing a GFN for a specific base is also $1/k$. On average this must be true, but because of various obvious relationships between bases, and correlations between factors for different bases such as those shown by Riesel [8], one might expect that each base has to be considered separately. However, we can make a plausible argument that the probability is always $1/k$, irrespective of the base b or the prime P .

First we note that divisibility of a number $F_{b,m}$ by a prime of the form (2) implies $b^{2^n} \equiv 1 \pmod{P}$. Conversely, if this relation holds for $b > 1$, an integer $m < n$ exists such that P divides $F_{b,m}$. This follows by induction from the fact that if some x satisfies $x^2 \equiv 1 \pmod{P}$, then x must equal $+1$ or -1 . Furthermore, by Fermat's little theorem, the prime P satisfies

$$(9) \quad (b^{2^n})^k \equiv 1 \pmod{P}$$

whenever $(b, P) = 1$. Here the value of b^{2^n} can only coincide with one of the k different k th roots of unity modulo P , one of which is 1. Assuming that the outcome of the computation of b^{2^n} modulo P behaves randomly, we can expect it to be 1 with probability $1/k$. But as we have seen, $b^{2^n} \equiv 1 \pmod{P}$ is equivalent to the existence of some $F_{b,m}$ divisible by P .

We decided to examine the assumption for particular bases by computer. Fortunately, extensive testing could be done because the second author maintains a comprehensive list of primes of the form $P(k, n)$, which is machine-readable [5]. As of October 1, 1992, this list consisted of all primes with the limits on k and n given in Table 2 (next page). The list had a total of 8,963 primes, including 36 miscellaneous primes beyond these limits. By summing $1/k$ over the entire list the expected value for the number of factors is 67.5.

We tested each of these primes to see how many were factors of GFNs for each of the bases from 2 to 15 which are not perfect powers. In general the test results appeared to confirm the theory, since the average number of factors per

TABLE 2. Prime table limits, October 1, 1992

| <i>k</i> -limits | | <i>n</i> -limits | |
|------------------|------|------------------|-------|
| from | to | from | to |
| 1 | 31 | 1 | 15000 |
| 33 | 63 | 1 | 12000 |
| 65 | 119 | 1 | 8000 |
| 121 | 211 | 1 | 4000 |
| 213 | 499 | 1 | 2500 |
| 501 | 1199 | 1 | 1000 |

base was 68.4. Testing each base required 3.1 hours, using a PC 486/33 with special-purpose number theory hardware [2].

4. TABLES OF FACTORS

The procedures for finding factors of generalized Fermat numbers are identical to those that have been used for many years for finding factors of standard Fermat numbers. Modern factoring methods are used for small values of m , trial division by appropriately sieved numbers $k \cdot 2^n + 1$, not necessarily prime, is used for small and medium values of n , and division by previously determined primes $P(k, n)$ is used for large values of n , where the residues required to decide on effective divisibility are obtained by repeated squarings modulo the possible factor (see also [6, p. 662]).

The division-by-prime method is particularly advantageous since any large primes, discovered while testing for factors for a particular base, can be added to the prime list [5] and are immediately available for testing other bases.

As a result of work done for this paper the prime list has been extended considerably. The search limits are shown in Table 3, and the largest primes, found for $3 \leq k \leq 31$, are presented in Table 4. The lower bounds for the searched ranges were suggested by previous work reported in the second part of [6]. The entire prime list consists of 133,253 primes, 8,476 of which have $n > 1000$. Since it took many thousands of hours over many years to find these primes, the usefulness of the prime list is obvious. It takes about 17.5 hours to determine which of these primes are factors for a particular base.

The expected value for the number of factors is about 91.3, and the real frequencies for the bases tested are shown in Table 5. Here the agreement between the expected value and the average number of factors is even more pronounced. The standard Fermat numbers (base 2), in particular, behave like GFNs for any other specific base. This observation can be of assistance to those searching for factors of Fermat numbers.

TABLE 3. New prime table limits

| <i>k</i> -limits | | <i>n</i> -limits | |
|------------------|-------|------------------|-------|
| from | to | from | to |
| 1 | 31 | 1 | 40000 |
| 33 | 63 | 1 | 12000 |
| 65 | 119 | 1 | 10000 |
| 121 | 219 | 1 | 8000 |
| 221 | 1199 | 1 | 4000 |
| 1201 | 2245 | 1 | 2000 |
| 2247 | 19999 | 1 | 1200 |

TABLE 4. Large new primes $P(k, n)$

| k | n -limits | | Primes found n |
|-----|-------------|-------|---|
| | from | to | |
| 3 | 21000 | 40000 | 34350 |
| 5 | 26000 | 40000 | 26607 |
| 7 | 16000 | 40000 | 16696, 22386 |
| 9 | 15000 | 40000 | 22603, 24422, 39186 |
| 11 | 15000 | 40000 | 15329, 18759, 28277 |
| 13 | 20000 | 40000 | 28280, 38008 |
| 15 | 15000 | 40000 | 19219, 21445, 21550, 24105, 24995, 34224, 34260 |
| 17 | 20000 | 40000 | |
| 19 | 15000 | 40000 | 17034, 23290 |
| 21 | 15000 | 40000 | 17524, 27124, 29769 |
| 23 | 20000 | 40000 | |
| 25 | 15000 | 40000 | |
| 27 | 15000 | 40000 | 19360, 30500, 38770 |
| 29 | 15000 | 40000 | 25723 |
| 31 | 20000 | 40000 | |

TABLE 5. Divisibility frequency for individual bases b

| b | number of factors |
|------------|----------------------|
| 2 | 78 |
| 3 | 100 |
| 5 | 106 |
| 6 | 74 |
| 7 | 94 |
| 10 | 104 |
| 11 | 88 |
| 12 | 96 |
| 13 | 85 |
| 14 | 74 |
| 15 | 102 |
| average = | 91.0 |
| expected = | 91.3 |

TABLE 6. Numbers $k \cdot 2^n + 1$ tested by trial division for bases 6, 10, 12

| n -limits | | k -limits |
|-------------|------|-------------|
| from | to | |
| 10 | 39 | 20000000 |
| 40 | 50 | 10000000 |
| 51 | 100 | 5000000 |
| 101 | 200 | 1000000 |
| 201 | 300 | 200000 |
| 301 | 400 | 100000 |
| 401 | 1000 | 20000 |

Tables 7, 8, and 9 (see pp. 402–404) are tabulations of the prime factors of base-6, base-10, and base-12 generalized Fermat numbers. The trial division limits are shown in Table 6. Unfortunately, all the trial divisions must be repeated for each base, but for these “small” divisors trial division still seems to be the most efficient procedure. The total CPU time used on a Siemens 7-890-F computer for the trial divisions (three bases) was about 780 hours.

TABLE 7. Prime factors $k \cdot 2^n + 1$ of base-6 Fermat numbers $6^{2^m} + 1$

| m | | n | k | | m | n | k | | m | n | k |
|-----|---|-----|------------------------|--------------|-----|-----|---------|--|-------|-------|--------|
| 0 | C | 1 | 3 | prime (7) | 33 | 35 | 21195 | | 201 | 202 | 7225 |
| 1 | C | 2 | 9 | prime (37) | 35 | 41 | 3 | | 203 | 209 | 3 |
| 2 | C | 4 | 81 | prime (1297) | | 40 | 2601 | | 244 | 247 | 237 |
| 3 | C | 4 | 1 | | | 36 | 60727 | | 261 | 262 | 55 |
| | | 4 | 6175 | | 36 | 41 | 21 | | 275 | 276 | 117007 |
| 4 | C | 5 | 11 | | 39 | 43 | 2517 | | 298 | 300 | 267 |
| | | 5 | 53 | | 40 | 41 | 191 | | 319 | 320 | 7 |
| | | 10 | 4599 | | | 43 | 567915 | | 342 | 346 | 26247 |
| 5 | C | 6 | 43 | | 42 | 43 | 9360659 | | 344 | 347 | 41139 |
| | | 6 | 2275 | | 44 | 45 | 8249 | | 370 | 371 | 5309 |
| | | 7 | 155117027389401 | | 47 | 48 | 712687 | | 373 | 374 | 1093 |
| 6 | C | 11 | 2405301 | | 50 | 51 | 1025 | | 380 | 382 | 105 |
| | | 7 | 3493619608100417 | | 56 | 57 | 509471 | | 389 | 390 | 7 |
| | | 7 | 224638962477005164271 | | 57 | 60 | 75 | | 403 | 405 | 16521 |
| 7 | C | 8 | 1 | | 61 | 62 | 9643 | | 431 | 432 | 7 |
| | | 8 | 2983 | | | 63 | 592491 | | 641 | 642 | 15295 |
| | | 8 | 196513 | | 63 | 65 | 9 | | 662 | 664 | 891 |
| | | 9 | 6232629 | | 64 | 67 | 9 | | 829 | 830 | 7 |
| | | 8 | 9138049087747333735 | | 66 | 67 | 8699 | | 1379 | 1384 | 81 |
| | | 10 | 2913113677352280802497 | | 78 | 80 | 357 | | 1420 | 1422 | 357 |
| | | 9 | 26-digits | | 79 | 83 | 2126397 | | 1675 | 1680 | 921 |
| 8 | | 11 | 9 | | 84 | 85 | 1169 | | 2294 | 2297 | 9 |
| 9 | | 10 | 79 | | 85 | 89 | 903 | | 2973 | 2974 | 43 |
| | | 11 | 1641 | | 92 | 93 | 955085 | | 2992 | 2993 | 185 |
| 10 | | 11 | 447425285 | | 96 | 97 | 341591 | | 3903 | 3904 | 25 |
| | | 13 | 45903 | | | 97 | 4160015 | | 4437 | 4438 | 19 |
| 11 | | 16 | 1472166285 | | 98 | 100 | 130893 | | 4542 | 4543 | 11 |
| 15 | | 16 | 1 | | | 100 | 2120097 | | 4642 | 4644 | 21 |
| 19 | | 20 | 13 | | 113 | 117 | 141 | | 4686 | 4687 | 5 |
| 21 | | 23 | 6292737 | | 118 | 119 | 136811 | | 4726 | 4727 | 29 |
| 22 | | 24 | 3484503 | | 126 | 127 | 5 | | 6341 | 6346 | 33 |
| 23 | | 24 | 2426623 | | | 127 | 11 | | 6801 | 6804 | 15 |
| 25 | | 26 | 37 | | 156 | 157 | 455585 | | 6978 | 6981 | 21 |
| | | 27 | 1137 | | 166 | 167 | 191 | | 7964 | 7967 | 9 |
| | | 28 | 4725 | | 179 | 180 | 211411 | | 9429 | 9431 | 9 |
| 27 | | 28 | 193 | | 187 | 188 | 13 | | 22385 | 22386 | 7 |
| 32 | | 35 | 1670619 | | 197 | 199 | 119361 | | | | |

Note: C means GFN is completely factored

Some of the factors for small m were taken from [1]. All the base-6 and base-10 factors in Riesel's paper [9] were rediscovered.

The total number of factors contained in Tables 7, 8, and 9 is 365. From the considerations leading to (7) the approximate frequencies of the differences $n - m$ occurring in a randomly chosen sample of 365 GFN factors can be predicted. The following is a comparison of the expected and actually counted frequencies:

| $n - m$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|----------|-----|----|----|----|----|---|---|---|---|
| Expected | 183 | 91 | 46 | 23 | 11 | 6 | 3 | 1 | 1 |
| Counted | 199 | 72 | 50 | 17 | 14 | 8 | 4 | | |

TABLE 8. Prime factors $k \cdot 2^n + 1$ of base-10 Fermat numbers $10^{2^m} + 1$

| m | | n | k | | m | n | k | m | n | k |
|-----|---|-----|----------------------|-------------|-----|-----|---------|-------|-------|-------|
| 0 | C | 1 | 5 | prime (11) | 29 | 31 | 135 | 226 | 227 | 1707 |
| 1 | C | 2 | 25 | prime (101) | 35 | 39 | 5 | 243 | 244 | 2661 |
| 2 | C | 3 | 9 | | 37 | 38 | 287443 | 260 | 262 | 19887 |
| | | 3 | 17 | | 39 | 40 | 52731 | 270 | 271 | 177 |
| 3 | C | 4 | 1 | | 40 | 41 | 21 | 284 | 291 | 701 |
| | | 4 | 367647 | | | 42 | 115 | 324 | 325 | 1283 |
| 4 | C | 5 | 11 | | 41 | 42 | 39 | 380 | 381 | 23 |
| | | 6 | 7 | | 48 | 52 | 25 | 388 | 389 | 101 |
| | | 7 | 5 | | 50 | 51 | 849 | 461 | 462 | 4963 |
| | | 7 | 11 | | 54 | 57 | 35535 | 550 | 552 | 9103 |
| | | 5 | 2183 | | | 57 | 3397839 | 615 | 616 | 7 |
| 5 | C | 7 | 155 | | 58 | 60 | 45 | 625 | 626 | 63 |
| | | 6 | 15253 | | 62 | 63 | 9 | 749 | 750 | 459 |
| | | 6 | 96679 | | 64 | 65 | 63 | 842 | 844 | 1273 |
| | | 7 | 6518964113895 | | 66 | 67 | 9 | 892 | 894 | 627 |
| 6 | C | 7 | 9882899 | | 68 | 69 | 15533 | 990 | 993 | 95 |
| | | 8 | 59934250737848194603 | | 69 | 70 | 21573 | 1104 | 1105 | 1551 |
| | | 7 | 31-digits | | 72 | 75 | 5 | 1147 | 1148 | 67 |
| 7 | C | 8 | 1 | | 80 | 83 | 1155045 | 1190 | 1191 | 299 |
| | | 10 | 15 | | 81 | 82 | 13 | 1286 | 1287 | 207 |
| | | 8 | 1771 | | 88 | 89 | 14603 | 1139 | 1141 | 1055 |
| | | 11 | 113-digits | | 91 | 93 | 4695 | 1370 | 1373 | 935 |
| 8 | C | 9 | 21 | | 93 | 94 | 1718239 | 1402 | 1403 | 539 |
| | | 9 | 16121 | | 99 | 100 | 3957 | 1628 | 1631 | 65 |
| | | 13 | 1162719 | | 102 | 104 | 43 | 1676 | 1677 | 123 |
| | | 9 | 142913093 | | | 105 | 460745 | 1919 | 1921 | 89 |
| | | 9 | 222-digits | | 122 | 125 | 755 | 1944 | 1947 | 5 |
| 9 | | 10 | 1479 | | 124 | 127 | 5 | 1960 | 1961 | 23 |
| | | 10 | 294999 | | 142 | 143 | 29 | 2686 | 2687 | 647 |
| 11 | | 13 | 13050269 | | 143 | 144 | 841 | 2731 | 2732 | 97 |
| | | 12 | 936342025557 | | | 149 | 3125 | 3306 | 3313 | 5 |
| | | 12 | 2203924854324541 | | 146 | 147 | 17 | 3353 | 3354 | 9 |
| 12 | | 13 | 56021 | | 157 | 158 | 43 | 3473 | 3474 | 273 |
| | | 13 | 88886432331741 | | 168 | 171 | 285 | 5147 | 5152 | 25 |
| 15 | | 16 | 1 | | 179 | 180 | 7 | 6612 | 6614 | 7 |
| | | 19 | 11 | | 181 | 183 | 679731 | 6837 | 6838 | 19 |
| 16 | | 17 | 63 | | 182 | 183 | 227 | 6903 | 6905 | 95 |
| 17 | | 19 | 335 | | 183 | 188 | 13 | 7926 | 7927 | 29 |
| 18 | | 21 | 305 | | 185 | 187 | 21 | 7966 | 7967 | 9 |
| 19 | | 20 | 67 | | 190 | 191 | 1637 | 9960 | 9961 | 113 |
| | | 21 | 101439 | | 195 | 201 | 154865 | 23467 | 23473 | 5 |
| | | 20 | 12838857 | | 200 | 202 | 267 | 28276 | 28277 | 11 |
| 20 | | 25 | 5 | | 206 | 207 | 87 | 38005 | 38008 | 13 |
| 22 | | 24 | 6061953 | | 208 | 209 | 3 | 44684 | 44685 | 3 |
| 26 | | 27 | 17 | | 215 | 216 | 143277 | | | |
| 29 | | 30 | 49 | | 222 | 225 | 64619 | | | |

Note: C means GFN is completely factored

During this investigation the first author discovered three new prime factors of standard Fermat numbers:

$$P(145, 7312) \mid F_{7309}, \quad P(11, 18759) \mid F_{18749}, \quad P(19, 23290) \mid F_{23288}.$$

A list of presently known factors is available from the second author .

TABLE 9. Prime factors $k \cdot 2^n + 1$ of base-12 Fermat numbers $12^{2^m} + 1$

| m | n | k | m | n | k | m | n | k |
|-----|-----|-------------------|-----|-----|---------|-------|-------|-------|
| 0 | C | 2 3 prime (13) | 26 | 30 | 327 | 408 | 409 | 113 |
| 1 | C | 2 1 | 29 | 30 | 49 | 485 | 486 | 283 |
| | | 2 7 | 30 | 32 | 63591 | 513 | 517 | 15 |
| 2 | C | 3 11 | 38 | 41 | 3 | 516 | 518 | 39 |
| | | 3 29 | 39 | 41 | 21 | 529 | 534 | 597 |
| 3 | C | 4 1 | 40 | 44 | 15 | 556 | 557 | 6965 |
| | | 5 3 | | 46 | 123 | 622 | 623 | 5525 |
| | | 4 16297 | | 43 | 318471 | 639 | 642 | 13245 |
| 4 | C | 5 4811 | 42 | 43 | 11 | 713 | 716 | 1233 |
| | | 5 37528551509 | 51 | 52 | 7 | 765 | 768 | 17031 |
| 5 | C | 8 3 | 56 | 57 | 6071 | 837 | 839 | 861 |
| | | 8 30-digits | 58 | 60 | 1125 | 966 | 972 | 957 |
| 6 | C | 8 141 | 63 | 64 | 26923 | 1010 | 1011 | 695 |
| | | 7 635 | 64 | 67 | 9 | 1052 | 1053 | 29 |
| | | 7 543905 | | 65 | 215735 | 1178 | 1179 | 299 |
| | | 10 71669658783177 | 66 | 70 | 1254537 | 1243 | 1245 | 609 |
| | | 8 33-digits | 68 | 69 | 4398833 | 1310 | 1312 | 57 |
| 7 | C | 8 1 | 86 | 89 | 81 | | 1313 | 1053 |
| | | 8 134-digits | 87 | 90 | 135 | 1348 | 1349 | 1781 |
| 8 | | 9 16121 | 91 | 92 | 7 | 1540 | 1541 | 113 |
| | | 9 576716099 | 97 | 98 | 817399 | 1803 | 1804 | 7 |
| 10 | | 11 3187781 | 99 | 100 | 200041 | 2288 | 2290 | 69 |
| 11 | | 12 421 | 126 | 127 | 5 | 2731 | 2733 | 21 |
| | | 12 1111 | | 127 | 1031 | 2811 | 2816 | 3 |
| | | 13 19473 | 127 | 129 | 158721 | 2814 | 2817 | 129 |
| 12 | | 13 5 | 129 | 133 | 22839 | 2872 | 2875 | 15 |
| | | 15 345 | 136 | 140 | 30153 | 3158 | 3165 | 129 |
| | | 13 9479 | 143 | 144 | 43 | 4343 | 4344 | 43 |
| 14 | | 15 5 | | 146 | 8019 | 4726 | 4727 | 29 |
| 15 | | 16 1 | 185 | 187 | 21 | 5946 | 5947 | 5 |
| 16 | | 18 1537305 | 202 | 204 | 2655 | 6999 | 7000 | 145 |
| 18 | | 19 11 | 204 | 211 | 9 | 7926 | 7927 | 29 |
| | | 19 41 | 207 | 209 | 3 | 8410 | 8411 | 41 |
| | | 20 141 | 215 | 216 | 31 | 9429 | 9431 | 9 |
| 19 | | 20 13 | 226 | 231 | 207 | 20906 | 20909 | 3 |
| | | 20 151 | 237 | 238 | 817 | 22601 | 22603 | 9 |
| | | 21 13011 | 307 | 308 | 13 | 26606 | 26607 | 5 |
| 21 | | 25 51 | 319 | 320 | 7 | 34222 | 34224 | 15 |
| | | 23 1140867 | 334 | 335 | 2495 | 42663 | 42665 | 3 |
| 23 | | 26 491997 | 351 | 353 | 3 | | | |

Note: C means GFN is completely factored

5. FUTURE STUDIES

As is very often the case, work done during the preparation of this article suggests related areas of research which should be pursued. Many noticeable deviations from statistical behavior have been observed empirically. For example, all the primes with $k = 3$ (except the smallest one, $P(3, 1) = 7$) divide a base-8 GFN, as is easily shown to be generally true. Other less evident regularities, like the following, should be investigated theoretically. Three-quarters of the known primes with $k = 3$ (actually, 19 out of 26) divide a base-3 GFN. Also, about half the primes with $k = 5$ (8 out of 18) divide a base-2 GFN and two-thirds of them (12 of the 18) divide a base-5 GFN.

Riesel in 1969 [8] cleverly derived a method for using factors of generalized Fermat numbers of one base to find factors for another base. For example, he shows that for $k = 5$, if a prime divides a base-2 GFN, it also divides a determined base-10 GFN. This work should be extended to obtain more stringent relationships.

In general, not enough attention has been paid to GFNs with odd bases. Although there has been some systematic searches for large GFN primes with even bases [3], very little has been done to find primes of the form $F_{b,m}/2$ for odd bases [7]. Also, finding factors of GFNs with odd bases is at least as interesting as finding factors of GFNs with even bases.

It is obvious that the existence of an extensive list of primes of the form (2) made the research for this paper practical. With the large and expanding number of high-performance workstations and PCs that are available to the academic community, it seems that a world-wide organized effort to expand this list would be a logical project.

ACKNOWLEDGMENT

We wish to thank Jeff Young for supplying us with new large primes, some of which are included as GFN factors.

BIBLIOGRAPHY

1. J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr., *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers*, 2nd ed., Contemp. Math., vol. 22, Amer. Math. Soc., Providence, RI, 1988.
2. C. Caldwell, *Review of the Cruncher PC plug-in board*, J. Recreational Math. **25** (1993), 56–57.
3. H. Dubner, *Generalized Fermat primes*, J. Recreational Math. **18** (1985–86), 279–280.
4. H. Griffin, *Elementary theory of numbers*, McGraw-Hill, New York, 1954.
5. W. Keller, *Table of primes of the form $k \cdot 2^n + 1$, k odd*, Hamburg, 1993 (unpublished).
6. ———, *Factors of Fermat numbers and large primes of the form $k \cdot 2^n + 1$* , Math. Comp. **41** (1983), 661–673; II (Preprint 27 September 1992).
7. M. Morimoto, *On prime numbers of Fermat type*, Sūgaku **38** (1986), 350–354. (Japanese)
8. H. Riesel, *Common prime factors of the numbers $A_n = a^{2^n} + 1$* , BIT **9** (1969), 264–269.
9. ———, *Some factors of the numbers $G_n = 6^{2^n} + 1$ and $H_n = 10^{2^n} + 1$* , Math. Comp. **23** (1969), 413–415.

449 BEVERLY ROAD, RIDGEWOOD, NEW JERSEY 07450

E-mail address: 70327.1170@compuserve.com

REGIONALES RECHENZENTRUM DER UNIVERSITÄT HAMBURG, 20146 HAMBURG, FEDERAL REPUBLIC OF GERMANY

E-mail address: keller@mailhost.rrz.uni-hamburg.de