MATHEMATICS OF COMPUTATION
Volume 67, Number 221, January 1998, Pages 441–446
S 0025-5718(98)00891-6

FACTORS OF GENERALIZED FERMAT NUMBERS

ANDERS BJÖRN AND HANS RIESEL

Abstract. A search for prime factors of the generalized Fermat numbers $F_n(a,b) = a^{2^n} + b^{2^n}$ has been carried out for all pairs (a,b) with $a,b \leq 12$ and $\text{GCD}(a,b) = 1$. The search limit k on the factors, which all have the form $p = k \cdot 2^m + 1$, was $k = 10^9$ for $m \leq 100$ and $k = 3 \cdot 10^6$ for $101 \leq m \leq 1000$. Many larger primes of this form have also been tried as factors of $F_n(a,b)$. Several thousand new factors were found, which are given in our tables.—For the smaller of the numbers, i.e. for $n \leq 15$, or, if $a,b \leq 8$, for $n \leq 16$, the cofactors, after removal of the factors found, were subjected to primality tests, and if composite with $n \leq 11$, searched for larger factors by using the ECM, and in some cases the MPQS, PPMPQS, or SNFS. As a result all numbers with $n \leq 7$ are now completely factored.

1. Generalized Fermat numbers

Generalized Fermat numbers (GFNs) of the form $F_n(a) = a^{2^n} + 1$ have been studied earlier by one of us, see [3], [4]. The access to fast computers has recently rekindled interest in these numbers [1]. Many of the properties of this particular type of numbers also hold for the slightly more general type $F_n(a,b) = a^{2^n} + b^{2^n}$ For obvious reasons we shall assume that a and b are lacking common divisors.

2. Properties of the factors of GFNs

The well-known theorem on the prime factors of the ordinary Fermat numbers $2^{2^n} + 1$ is in the more general case replaced by the following result.

Theorem 2.1. *Suppose that $p = k \cdot 2^m + 1 | F_n(a,b)$, with k odd, and that $u \equiv a/b \bmod p$ is a 2^t-power residue but not a 2^{t+1}-power residue* $\bmod p$. *Then $m = n + t + 1$.—If u is not even a quadratic residue, we have to put $t = 0$.*

Proof. We know that $a^{2^n} + b^{2^n} \equiv b^{2^n}(u^{2^n} + 1) \equiv 0 \bmod p$. Since $u \equiv x^{2^t}$ for some x, $-1 \equiv u^{2^n} \equiv (x^{2^t})^{2^n} = x^{2^{n+t}} \bmod p$. Suppose that $x \bmod p$ belongs to the exponent $d = (p-1)/l = k \cdot 2^m/l$. Then $x^{d/2} \equiv -1 \bmod p$, and $d/2$ is also the *smallest* positive exponent, yielding -1. Therefore $d = 2^{n+t+1}$, $l = k \cdot 2^m/d = k \cdot 2^{m-n-t-1}$, and $m \geq n + t + 1$. Since we have presumed that u is a 2^t-power residue, but not a 2^{t+1}-power residue, x is a quadratic non-residue, and thus $x^{(p-1)/2} \equiv -1 \bmod p$. Thus, $(p-1)/2$ must be an *odd* multiple of $d/2$ and thus $l = (p-1)/d$ is odd, which implies that $m - n - t - 1 = 0$. Thus m is in this case *exactly* $n + t + 1$. □

Received by the editor May 6, 1996 and, in revised form, September 19, 1996.
1991 *Mathematics Subject Classification.* Primary 11-04, 11A51, 11Y05, 11Y11.
Key words and phrases. Fermat numbers, primes, factorization.

©1998 American Mathematical Society

3. Alternative formulation

Since a/b is a quadratic residue at the same time as ab is, and a biquadratic residue if and only if ab^3 is, *etc.*, the above criterion can be replaced by the following set of conditions:

If ab is a quadratic residue $\bmod p$, then $m \geq n+2$,
if ab^3 is a biquadratic residue $\bmod p$, then $m \geq n+3$,
if ab^7 is an octic residue $\bmod p$, then $m \geq n+4$,
and so on.

4. Application of the theorem

In some simple cases a/b is always at least a quadratic residue $\bmod p$ for all possible prime factors of $F_n(a,b)$, which implies that $m \geq n+2$. Such cases are given by the ordinary Fermat numbers, a fact which has long been known, and e.g. the cases $(a,b)=(9,2)$ and $(9,8)$, since 2 and thus also 18 and 72 are quadratic residues of all primes $\equiv 1 \bmod 8$. The theorem also explains, in a natural way, the statistics which have been gathered, by us and by other authors, on the frequency of the values of $m-n$. Since there are half as many 2^{t+1}-power residues $\bmod p$ as there are 2^t-power residues, the theorem explains the observed falling off by a factor 2 when $m-n$ is augmented by 1.

5. The number of primes $k \cdot 2^m + 1$ in a rectangular domain

When searching for primes it may be interesting to know approximately how many primes you can expect to find. Now, every prime p has the form $k \cdot 2^m + 1$ for some m and some odd number k, both uniquely determined. For $m=1$ we find the primes $p=(2a+1)\cdot 2^1+1=4a+3$, for $m=2$ we have the primes $p=(2a+1)\cdot 2^2+1=8a+5$, and so on. To obtain the number of primes G for $k \leq K$ and $\mu \leq m \leq M$ we have to count the number of primes in each of a number of arithmetic series:

$$\begin{aligned}G(K) &= \pi_{2^{\mu+1},2^{\mu}+1}(K\cdot 2^{\mu}+1)+\pi_{2^{\mu+2},2^{\mu+1}+1}(K\cdot 2^{\mu+1}+1)\\ &\quad+\ldots+\pi_{2^{M+1},2^{M}+1}(K\cdot 2^{M}+1)\\ &\approx \sum_{m=\mu}^{M}\frac{\pi(2^m K)}{2^m},\end{aligned}$$

according to Dirichlet's theorem. This can be further approximated by the prime number theorem, which we here use in the form $\pi(x) \asymp x/(\log x - 1)$ in order to achieve a slightly better approximation for moderate values of x:

$$\begin{aligned}G(K) &\approx \sum_{m=\mu}^{M}\frac{K}{\log(2^m K)-1}=\sum_{m=\mu}^{M}\frac{K}{m\log 2+\log K-1}\\ &\approx \int_{\mu-1/2}^{M+1/2}\frac{K\,dx}{x\log 2+\log K-1}=\frac{K}{\log 2}\big[\log(x\log 2+\log K-1)\big]_{x=\mu-1/2}^{M+1/2}.\end{aligned}$$

6. Statistics gathered on prime factors of GFNs

According to the divisibility theory of GFNs, presented in [1], which is immediately applicable also to our case $F_n(a,b)$, with $b \neq 1$, a prime factor $p = k \cdot 2^m + 1$, with k odd, divides some F_n for the proportion $1/k$ of all combinations of a and b. Thus the total number of factors with $\mu \leq m \leq M$ and $\kappa \leq k \leq K$ (k odd), for the GFNs, generated by some fixed combination of a and b, is expected to be (k is odd in the summations below)

$$\sum_{m=\mu}^{M}\sum_{k=\kappa}^{K}\frac{2}{k\log 2^m k}=\sum_{k=\kappa}^{K}\sum_{m=\mu}^{M}\frac{1}{k}\frac{2}{m\log 2+\log k}\approx\sum_{k=\kappa}^{K}\int_{\mu-1/2}^{M+1/2}\frac{1}{k}\frac{2\,dx}{x\log 2+\log k}$$

$$=\frac{2}{\log 2}\sum_{k=\kappa}^{K}\frac{1}{k}\log\frac{(M+\frac{1}{2})\log 2+\log k}{(\mu-\frac{1}{2})\log 2+\log k}\qquad(\text{with } k=2k'+1)$$

$$=\frac{2}{\log 2}\sum_{k'=(\kappa-1)/2}^{(K-1)/2}\frac{1}{2k'+1}\log\frac{(M+\frac{1}{2})\log 2+\log(2k'+1)}{(\mu-\frac{1}{2})\log 2+\log(2k'+1)}$$

$$\approx\frac{2}{\log 2}\int_{\kappa/2-1}^{K/2}\log\frac{(M+\frac{1}{2})\log 2+\log(2t+1)}{(\mu-\frac{1}{2})\log 2+\log(2t+1)}\frac{dt}{2t+1}\qquad(\text{with } u=2t+1)$$

$$=\frac{1}{\log 2}\int_{\kappa-1}^{K+1}\log\frac{(M+\frac{1}{2})\log 2+\log u}{(\mu-\frac{1}{2})\log 2+\log u}\frac{du}{u}$$

$$=\Bigg[\frac{\log u}{\log 2}\log\frac{(M+\frac{1}{2})\log 2+\log u}{(\mu-\frac{1}{2})\log 2+\log u}+\left(M+\tfrac{1}{2}\right)\log\left(\left(M+\tfrac{1}{2}\right)\log 2+\log u\right)$$
$$-\left(\mu-\tfrac{1}{2}\right)\log\left(\left(\mu-\tfrac{1}{2}\right)\log 2+\log u\right)\Bigg]_{u=\kappa-1}^{K+1}.$$

The summation formula used here is a two-dimensional version of a certain variation of the Euler–MacLaurin sum formula, shown in $G(K)$ above. See [2], [6].

The authors have gathered statistics on all factors in the searched domain, for $m \geq 11$ and $k < 10^s$, $s = 3, 4, \ldots, 9$ up to $m = 1000$. Here we give the average values of the number of factors found for each combination (a, b) compared with the estimated values from the formula given above

$11 \leq m \leq 100$	$k < 10^3$	$< 10^4$	$< 10^5$	$< 10^6$	$< 10^7$	$< 10^8$	$< 10^9$
Minimum	13	15	20	24	26	30	32
Maximum	30	34	41	48	53	55	58
Average	19.39	24.93	29.85	34.56	39.10	43.29	47.10
Formula	19.29	24.69	29.72	34.43	38.87	43.07	47.06

$101 \leq m \leq 1000$	$k < 10^3$	$< 10^4$	$< 10^5$	$< 10^6$
Minimum	9	11	17	21
Maximum	33	40	51	64
Average	20.29	26.83	32.98	40.76
Formula	22.47	29.78	37.01	44.14

As can be seen from the above comparison, our formula "overshoots" the counted number of factors, for the larger values of m. This is probably due to some effect of counting only a small number of primes at the beginning of each of the arithmetic series involved, which might invaluate Dirichlet's theorem as a good approximation to the actual number of primes in a rectangular domain.

7. How the factor tables are organized

For each pair (a, b), with $1 \le b < a \le 12$, and $\mathrm{GCD}(a, b) = 1$, except for the pairs $(2,1)$, $(4,1)$, and $(9,4)$, all known prime factors of the GFNs are given for $4 \le n \le 999$. Also, many of the larger known primes of the form $k \cdot 2^m + 1$ have been tried and recorded as factors. The pairs $(4,1)$ and $(9,4)$ are excluded because the numbers are the same as for $(2,1)$ and $(3,2)$, respectively, for the next value of n. For the pair $(8,1)$ the factors in the tables refer instead to the number $(8^{2^n}+1)/(2^{2^n}+1) = 4^{2^n} - 2^{2^n} + 1$. In Table 1, all factors of the form $p = k \cdot 2^m + 1$ in the following range are given explicitly, by writing each factor in this very form:

$$\begin{array}{rcccrl}
1 & < & m & \le & 100, & k < 10^9 \\
100 & < & m & \le & 1000, & k < 3 \cdot 10^6 \\
1000 & < & m & \le & 3000, & k < 21000 \\
3000 & < & m & \le & 5000, & k < 10000 \\
5000 & < & m & \le & 10000, & k < 1200 \\
10000 & < & m & \le & 12000, & k < 220 \\
12000 & < & m & \le & 20000, & k < 120 \\
20000 & < & m & \le & 50000, & k < 64 \\
50000 & < & m & \le & 100000, & k < 32
\end{array}$$

Larger factors of $F_n(a, b)$, for $n \le 12$, which however have not been systematically searched for, are indicated by their number of digits as Pxx, or as $PRPxx$, if their primality has not yet been proved. For xx up to 100, these factors can be looked up in the supplementary tables, Table 2. The last prime factor in each decomposition has been marked with an asterisk (*) to indicate that the corresponding number $F_n(a, b)$ has been completely factored. Only three of the *PRP*s, all with more than 1000 digits, have not yet been proven primes. All numbers with $n \le 7$ have been completely factored, and all cofactors with less than 60,000 digits have been subjected to strong primality tests.—Tables are included in the microfiche supplement at the back of this issue.

8. A time saving device

As we have remarked already in our preliminary report [5] on this project, we computed only the values of $a^{2^n} \bmod p$ for the 9 values $a = 4$ to $a = 12$, and combined these residues to find the residues $\bmod p$ for the interesting 41 pairs under study. For $m > 1000$ we further saved computing time by avoiding to perform divisibility tests for $n < m - 50$. Thanks to this we could restrict ourselves to compute the residues for only the five values of $a = 4$, 5, 7, 9, and 11 (the five primes < 12 would also have worked), i.e. we calculated $a^{2^{m-50}} \bmod p$ for these values of a. We could then find the corresponding residues for $a = 6$, 8, 10, and 12 by using only 4 multiple precision multiplications. For the last 50 steps we proceeded as previously described, working with all 9 residues. To ascertain that not some factor p with $n < m - 50$ escaped our notice, we checked that $a^{2^{m-50}} \not\equiv b^{2^{m-50}} \bmod p$.— The largest difference found for any $m - n$ was 14, which occurred for the factor $35 \cdot 2^{47} + 1$ of $F_{33}(7, 5)$.

9. Largest factor found with ECM

In searching for factors larger than our search limits, we employed a version of ECM, graciously put at our disposal by Richard Brent. The largest factor found was the factor $P33$ of the cofactor $C135$ of $F_8(5,3)$, after a couple of smaller factors had been removed.—Some of the larger cofactors, which did not yield to attacks with ECM, were factored by MPQS, PPMPQS, or SNFS. The largest of these were cofactors of $11^{128}+4^{128}$ and $12^{128}+5^{128}$, both C131.

10. Search for multiple factors

All prime factors found with less than 4000 decimal digits have been tested as possible square factors. No large square factor was found. Only the following small multiple factors were found: The obvious 5^2 in 4^2+3^2 and in 7^2+1, 5^3 in 11^2+2^2, 13^2 in 12^2+5^2, and, finally, the less obvious 17^2 in 9^8+7^8 and in 11^8+4^8.

The occurrence of multiple factors is governed by the following line of reasoning: Any prime $p = k\cdot 2^m+1$ divides one GFN for roughly $1/k$ of all combinations of a and b. Using the theory of congruences, it is easy to deduce that p^2 divides one GFN for roughly $1/kp$, and p^3 divides one GFN for roughly $1/kp^2$, etc. of all pairs (a,b). Starting with a factor p of some $F_n(a,b)$ it is easy to construct a new pair (a,b) with some GFN divisible by p^2, from this one another pair with some GFN divisible by p^3, etc. Here is an example: Starting from $641|5^{32}+4^{32}$, we first solve the *linear* congruence $4^{32}+(5+641x)^{32}\equiv 0 \bmod 641^2$, or $(4^{32}+5^{32})/641 \equiv -32\cdot 5^{31}x \bmod 641$, yielding $x\equiv -137$ and thus $641^2|4^{32}+(5-137\cdot 641)^{32} = 4^{32}+87812^{32}$. Next, we solve $4^{32}+(87812+641^2y)^{32}\equiv 0 \bmod 641^3$, or $(4^{32}+87812^{32})/641^2 \equiv -32\cdot 87812^{31}y \bmod 641$, with $y\equiv -85$, and so $641^3|4^{32}+(87812-85\cdot 641^2)^{32} = 4^{32}+34837073^{32}$, and so on. A handier example, starting from $641^2|177^{64}+4^{64}$, found by search for small solutions to $641^2|x^{64}+y^{64}$, successively gives $641^3|68617304^{64}+4^{64}$, $641^4|63541925065^{64}+4^{64},\dots$

The number of square prime factors expected in the region investigated is actually quite small. An estimation of the number of factors p^2, dividing a given combination of a and b for all $m\geq 5$ and $k\geq 1$, would be:

$$\sum_{m=5}^{\infty}\sum_{k=1}^{\infty}\frac{1}{k(k\cdot 2^m+1)\log 2^m k} < \sum_{k=1}^{\infty}\frac{1}{k^2}\sum_{m=5}^{\infty}\frac{1}{2^m(m\log 2+\log k)}$$

$$< \sum_{k=1}^{\infty}\frac{1}{k^2}\sum_{m=5}^{\infty}\frac{1}{2^m m\log 2} = \frac{\pi^2}{6}\sum_{m=5}^{\infty}\frac{1}{2^m m\log 2} = \frac{\pi^2}{6}\cdot 0.016 = 0.026.$$

This may explain, why no "large" squared prime factors have been found in any ordinary or generalized Fermat number so far.

Acknowledgements

The authors are indebted to David Bailey and NASA Ames for letting them use MPFUN, and to the following persons for kind and most valuable assistance during different stages of this project: Henk Boender, Richard Brent, Harvey Dubner, Marije Huizing, Wilfrid Keller, Peter L. Montgomery, François Morain, Herman te Riele, Thomas Sosnowski, Jeff Young, and an anonymous referee.—Linköping University has graciously supported this project by putting idle computing time at our disposal.

References

1. H. Dubner and W. Keller, *Factors of Generalized Fermat Numbers,* Math. Comp. **64** (1995), 397–405. MR **95c:**11010
2. E. Lindelöf, *Le Calcul des Résidus et ses Applications a la Théorie des Fonctions,* Gauthier-Villars, Paris 1905, formula (3) on p. 78.
3. H. Riesel, *Some Factors of the Numbers $G_n = 6^{2^n} + 1$ and $H_n = 10^{2^n} + 1$,* Math. Comp. **23** (1969), 413–415. MR **39:**6813
4. H. Riesel, *Common Prime Factors of the Numbers $A_n = a^{2^n} + 1$,* BIT **9** (1969), 264–269. MR **41:**3381
5. H. Riesel and A. Björn, *Generalized Fermat Numbers,* in *Mathematics of Computation 1943–1993: A Half-Century of Computational Mathematics,* W. Gautschi, ed., Proc. Symp. Appl. Math. **48** (1994), 583–587, Amer. Math. Soc., Providence, R.I., 1994. MR **95j:**11006
6. H. Riesel, *Summation of Double Series Using the Euler–MacLaurin Sum Formula,* BIT **36** (1996), 860–862. CMP 97:04

Department of Mathematics, Linköping University, S-581 83 Linköping, Sweden
E-mail address: `anbjo@mai.liu.se`

Department of Numerical Analysis and Computing Science, Royal Institute of Technology, S-100 44 Stockholm, Sweden
E-mail address: `riesel@nada.kth.se`