Elemente der Mathematik (Online first)
DOI 10.4171/EM/522

Published by EMS Press

Six primes in generalized Fermat numbers

Gerold Brändli and Jörg Waldvogel

Gerold Brändli, born 1939, obtained his Ph.D. from ETH Zürich in experimental physics, was a postdoc at Cornell University, USA, and worked then in Swiss companies, e.g. in the development of liquid crystal displays, and finally taught until 2005 mathematics at a high school.

Jörg Waldvogel received his Ph.D. in mathematics from ETH Zürich in 1966. As of 1973, after positions as research scientist and as assistant professor in Huntsville, Alabama and Austin, Texas, he held positions at ETH, first as the head of the Numerical Analysis Group, later as a professor, until his retirement in 2003. His research interests are concrete mathematics, in particular numerical mathematics, celestial mechanics, and number theory.

1 Introduction and definitions

This section refreshes some basic knowledge about the Fermat numbers and defines the generalization used in this paper.

The mathematician Pierre de Fermat introduced the integers $F_n = 2^{2^n} + 1$ ($n \geq 0$) and conjectured them all to be prime. Euler found a divisor of F_5, namely 641. Since then, the Fermat numbers beyond the first five primes $\{3, 5, 17, 257, 65\,537\}$ have been widely

Der Mönch Marin Mersenne und der Jurist Pierre de Fermat traten 1636 unter anderem über Zahlentheorie in Briefkontakt. Sie brachten dabei je eine Zahlenfolge zur Diskussion, die Primzahlen enthalten, nämlich die heute nach ihnen benannten Mersenne-Zahlen $M_n = 2^n - 1$ und die Fermat-Zahlen $F_n = 2^{2^n} + 1$. Die Mersenne-Zahlen sind häufig prim. Unter den Fermat-Zahlen sind aktuell nur fünf Primzahlen bekannt. Deshalb verallgemeinerte man die Fermat-Zahlen beispielsweise zu $F_{b,n} = b^{2^n} + 1$ ($b > 2$ eine gerade Zahl). Mit modernen Methoden fand man in den Folgen M_n und $F_{b,n}$ immer wieder sehr grosse Primzahlen, z. B. 2022 eine mit über sechs Millionen Ziffern: $F_{1963736,20} = 1963736^{2^{20}} + 1$. Leonhard Euler zeigte, dass die sechste Fermat-Zahl durch 641 teilbar ist. Seither wurden für fast dreissig Fermat-Zahlen Faktoren gefunden. Man vermutet, dass tatsächlich nur die ersten fünf Fermat-Zahlen prim sind. In der vorliegenden Arbeit wurden bei den Zahlen $F_{b,n}$ die Parameter b gesucht, die ebenfalls fünf Primzahlen ergeben. Überraschend wurden dabei vier Fälle mit sechs Primzahlen gefunden. Kann man daraus etwas für die genannte Vermutung ableiten?

studied. The existence of a *sixth prime* is very improbable [2], but its non-existence is not yet proven.

There exist several ways to generalize the Fermat numbers. A simple one is described by Dubner and Gallot [4] as follows.

Definition 1.1. *Generalized Fermat Numbers (GFN)* are defined as

$$F_{b,n} = b^{2^n} + 1,$$

b a positive integer and $n \geq 0$. In the search for primes, one can additionally require b to be even and not to be the square of a lesser b, to avoid a double visit of the same GFN.

This definition of GFN includes with $b = 2$ the Fermat primes.

In the search for very large primes, Mersenne numbers of the form $2^n - 1$ (see [6]) and Fermat numbers are in the focus of the specialists. During many years, Mersenne numbers were easier to factorize. In 1994, R. Crandall and B. Fagin discovered the Discrete Weighted Transforms to speed up the multiplication and applied it to Mersenne numbers. Around 1998, Dubner and Gallot remarked that the new method is also applicable to Fermat numbers and even to GFN [4]. Since then, many new large primes have been found [8]. At present, the largest known primes are Mersenne numbers, followed by the not so known Proth numbers of form $k\,2^e + 1$ (see [7]), and then by GFN.

The focus of this paper is to count the number of primes in GFN for fixed b, and it shows what can be done using more traditional software.

The $F_{b,n}$ have – like the Fermat numbers – a double exponentiation; they grow very fast. The writing $b^{2^n} + 1$ is used instead of more general $b^e + 1$ with integer $e > 0$ to skip composites on the search for prime $F_{b,n}$.

Theorem 1.2. *Let b be a positive even number and e a positive integer greater than* 1*, but* not a power of 2*; then* $b^e + 1$ *is composite.*

Proof. Let the exponent e be written as a binary number; then each digit 1 corresponds to a divisor b^{2^k} of b^e. And let kmin denote the least such k; then $b^{2^{\text{kmin}}} + 1$ is a divisor of any $b^e + 1$. Therefore, more than one digit 1 in the binary number implies $b^e + 1$ to be composite. ∎

Definition 1.3. The sequence $S(b)$ is defined as

$$S(b) = \{F_{b,n} \text{ with integer } n \geq 0\}.$$

Sequences $S(b)$ with at least five primes are numbered by k.

2 Sequences $S(b)$ with five or six primes

For practical reasons – computing time and upper limit of *isprime* function –, only $b < 1.5 \cdot 10^9$ were completely studied, additionally few examples up to $b < 10^{26}$. As result, more than 500 sequences $S(b)$ with *five primes* were found. Here are the first 60.

k	b	$n_1,\ldots,n_5$	$T(b)$	k	b	$n_1,\ldots,n_5$	$T(b)$
1	2	0, 1, 2, 3, 4	—	31	17 702 106	0, 1, 2, 4, 8	24.4
2	2 926	0, 1, 3, 4, 9	3.2	32	18 914 850	0, 2, 3, 4, 9	25.3
3	77 140	0, 1, 2, 4, 9	3.9	33	19 350 688	0, 2, 3, 4, 6	25.7
4	137 650	1, 2, 3, 4, 6	4.2	34	19 862 714	1, 2, 3, 4, 6	26.1
5	337 536	0, 1, 2, 3, 4	5.0	35	20 706 120	0, 1, 2, 3, 4	26.7
6	550 630	0, 2, 3, 5, 6	5.6	36	21 925 150	0, 1, 2, 5, 7	27.6
7	585 106	0, 1, 2, 3, 4	5.7	37	25 038 400	0, 1, 2, 3, 9	30.0
8	602 056	0, 1, 2, 3, 4	5.7	38	25 653 136	0, 2, 3, 4, 5	30.4
9	2 071 960	0, 1, 2, 3, 4	8.5	39	26 661 646	0, 1, 3, 4, 5	31.2
10	2 090 676	1, 2, 3, 4, 5	8.5	40	26 923 886	2, 3, 5, 7, 10	31.4
11	2 379 240	0, 1, 4, 5, 8	9.0	41	32 522 910	0, 1, 2, 4, 6	35.2
12	3 394 606	0, 1, 2, 4, 6	10.4	42	32 885 620	0, 2, 3, 4, 5	35.4
13	4 325 730	0, 1, 2, 4, 8	11.6	43	33 222 152	2, 3, 4, 5, 6	35.7
14	4 457 446	0, 1, 2, 4, 5	11.8	44	41 525 380	0, 1, 2, 4, 5	41.0
15	4 484 610	0, 1, 2, 4, 10	11.8	45	41 704 248	0, 2, 3, 4, 5	41.1
16	5 081 980	0, 1, 2, 4, 5	12.5	46	49 575 022	0, 1, 2, 3, 4	45.9
17	5 594 836	0, 1, 2, 4, 6	13.1	47	53 183 770	0, 1, 3, 6, 7	48.1
18	5 738 496	0, 1, 2, 5, 9	13.3	48	54 020 170	0, 1, 2, 3, 4	48.5
19	8 919 550	0, 1, 2, 4, 9	16.6	49	58 306 668	0, 2, 3, 4, 5	51.0
20	9 255 066	0, 2, 4, 7, 8	17.0	50	60 181 860	1, 2, 4, 5, 9	52.1
21	9 616 612	0, 2, 3, 4, 5	17.3	51	60 453 520	0, 1, 2, 4, 6	52.2
22	10 698 706	0, 2, 4, 5, 6	18.4	52	62 955 688	0, 2, 3, 5, 6	53.6
23	11 815 486	0, 2, 4, 5, 8	19.4	53	68 321 556	0, 2, 3, 4, 7	56.6
24	11 837 826	0, 1, 2, 4, 6	19.4	54	68 615 860	0, 2, 3, 4, 6	56.7
25	11 861 410	0, 1, 2, 3, 4	19.4	55	71 467 216	0, 1, 3, 4, 6	58.3
26	12 603 498	0, 2, 3, 4, 5	20.1	56	75 329 620	0, 1, 3, 4, 5	60.3
27	13 070 076	0, 1, 3, 4, 5	20.5	57	76 192 228	0, 2, 3, 4, 6	60.8
28	14 073 706	0, 1, 2, 4, 5	21.4	58	76 710 916	0, 1, 2, 4, 6	61.0
29	15 438 300	0, 1, 2, 5, 6	22.5	59	79 194 232	0, 2, 4, 5, 7	62.3
30	17 640 486	0, 1, 2, 4, 6	24.3	60	87 155 040	0, 1, 2, 3, 5	66.4

Table 1. The first 60 sequences $S(b)$ with at least *five primes* $F_{b,n_1}, F_{b,n_2}, F_{b,n_3}, F_{b,n_4}, F_{b,n_5}$. The number $T(b) = 1.038 \int_2^b dt/\ln(t)^5$ $(b > 2)$ is defined in Section 3.

The first example ($k = 1$) are the Fermat primes $F_{2,n}$ with $n = \{0, 1, 2, 3, 4\}$. The requirement in Definition 1.1 that b must not be the power of a lesser b excludes fewer than one in thousand b; it avoids to count a GFN a second time. Although the data of Table 1 comprise only the first 60 examples, they represent the 500 studied sequences quite well. The largest prime in Table 1 is in $k = 40$ with $b = 26\,923\,886$ and $F_{b,10} \approx 10^{7608.46}$.

Remarks. To keep the computing time low, we often limited the index to $n \leq 10$ and skipped by this measure a few examples. Astonishing results are that $n_j = 3$ (35×) is in Table 1 less frequent than $n_j = 4$ (51×), or that $n = \{0, 1, 2, 3, 4\}$ exists only 9× instead of the expected 20×. More details about these remarks follow in Section 3.

As a surprise, four sequences were found with *six primes*:

k	b	n_1	n_2	n_3	n_4	n_5	n_6	$T(b)$
152	292 582 836	0	1	2	3	4	7	152.8
175	377 434 326	0	1	2	5	6	10	183.0
468	1 381 729 444	1	2	4	6	8	9	469.9
approx. 3 350	19 388 732 416	0	1	3	6	8	9	3 352.1

Table 2. The four sequences $S(b)$ found with *six primes* $F_{b,n_1}, F_{b,n_2}, F_{b,n_3}, F_{b,n_4}, F_{b,n_5}, F_{b,n_6}$. The last k is an approximation because the $S(b)$ in-between where not studied throughout.

The large k on the last line suggests that there exist many more $S(b)$ with six primes. The b-numbers in Table 2 do not exhibit any obvious mathematical property.

To do the calculations, we used the software PARI/GP and Maple on standard computers and invested about 3000 computing hours. The largest prime encountered is $F_{b,12} \approx 10^{20883.19}$ with $b = 125\,440$. The function *isprime* in PARI/GP takes (depending on the computer) 3 to 15 minutes to test its primality.

3 Theoretical approach to k

The theoretical approach to k presented in this section is based on and shows similarity to the *prime number theorem*. This states that the number of primes not exceeding x grows asymptotically like

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\ln(t)} \quad (x \geq 2)$$

(see e.g. [1] or [5]). The derivation $d/dx\,\mathrm{Li}(x) = 1/\ln(x)$ $(x \geq 2)$ implies that a good approximation of the probability of x to be prime is

$$w(x) = 1/\ln(x).$$

An often cited consequence is that the squaring of x to x^2 halves the probability, i.e. $w(x^2) \approx w(x)/2$, which is a good thumb rule for natural numbers x. But for the constructed numbers $F_{b,n}$ (Definition 1.1), one gets for small n big deviations, i.e.

$$w(F_{b,n+1}) \neq w(F_{b,n})/2 \quad (n+1 \text{ means an additional squaring of } b).$$

The following two theorems give an explanation for this fact.

Theorem 3.1. *Any two numbers in* $S(b)$ *are* relatively prime.

Proof. Let $F_{b,n} = b^{2^n} + 1$ and $F_{b,n+k} = b^{2^{n+k}} + 1$ $(k > 0)$ be any two numbers. Suppose that m is a positive integer such that $m \mid F_{b,n}$ and $m \mid F_{b,n+k}$. Setting $x = b^{2^n}$, we have

$$\frac{F_{b,n+k} - 2}{F_{b,n}} = \frac{x^{2^k} - 1}{x + 1} = x^{2^k - 1} - x^{2^k - 2} + \cdots - 1$$

so that $F_{b,n} \mid (F_{b,n+k} - 2)$. It follows that $m \mid (F_{b,n+k} - 2)$. Since m also divides $F_{b,n+k}$, this implies that $m \mid 2$. But $F_{b,n}$ and $F_{b,n+k}$ are odd. Therefore, $m = 1$, which proves the theorem. This is an adapted version of Polyas' proof for Fermat numbers (see [3]). ∎

Therefore, a once used prime factor cannot be used a second time at higher n. This increases the probability of $F_{b,n}$ to be prime. The next theorem has a very big influence on the distribution of primes in GFN.

Theorem 3.2. *The* prime factors *of $F_{b,n}$ are of the form $2^{n+1}u + 1$ (u a positive integer).*

Proof. Let p be a divisor of $F_{b,n}$ (b is even!); then

$$b^{2^n} \equiv -1 \pmod{p}.$$

Squaring, we obtain $b^{2^{n+1}} \equiv 1 \pmod{p}$. It follows that 2^{n+1} is the smallest positive integer e such that $b^e \equiv 1 \pmod{p}$, so b has order 2^{n+1} modulo p. The full multiplicative group of integers modulo p has order $p - 1$. The order of any element divides the order of the group, so 2^{n+1} divides $p - 1$. Equivalently, p is of the form $2^{n+1}u + 1$. (A proof according to Gauss and Lukas.) ∎

This theorem excludes prime factors at most $2^{n+1} + 1$ and delivers a hint why Fermat primes F_n often divide GFN.

As an example, one can conclude from Theorem 3.2 that, in 17 consecutive b-numbers, there are exactly eight $F_{b,3}$, four $F_{b,2}$, two $F_{b,1}$, and one $F_{b,0}$ divisible by $F_2 = 17$, and two b are without this divisor. Analog statements are possible for all Fermat primes.

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13
times	471	426	433	302	380	244	164	72	98	59	23	(12)	(6)	(3)

Table 3. The frequencies of the index n in the 500 b found with at least 5 primes. The numbers in brackets are estimated.

The divisibility of GFN by Fermat primes spreads quite remarkably the numbers in Table 3, and it explains why $n = 4$ (380×) occurs more often than $n = 3$ (302×). Similarly, $n = 8$ is more frequent than $n = 7$. Above $n = 8$ and far away from the last Fermat prime, the rule $w(F_{b,n+1}) = w(F_{b,n})/2$ should be applicable. It allows to estimate the numbers in brackets, the missed b by our limit $n \le 10$.

The next definition is an analytical approximation to the counting numbers k.

Definition 3.3. Approximating $b^j + 1$ by b^j and assuming $w(F_{b,n})$ to be proportional to $1/\ln(b)$ (with unknown factor), then the expected number of sequences $S(b)$ with at least five primes is defined as

$$T(b) = c \int_2^b \frac{dt}{\ln(t)^5} \quad (c = 1.038,\ b > 2).$$

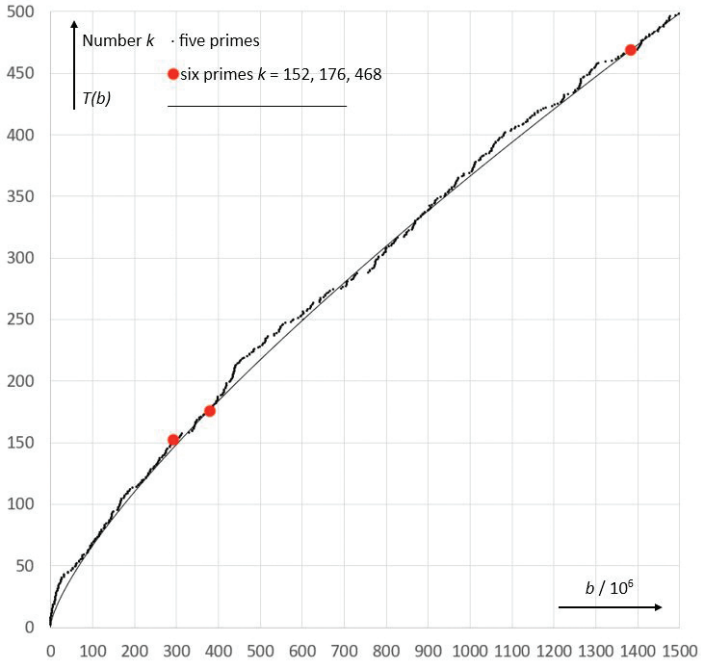

Figure 1. The sequences $S(b)$ numbered by k with five (·) or six (•) primes and $T(b)$ (—) (Definition 3.3), up to $b = 1500 \cdot 10^6$.

The number $T(b)$ is defined in analogy to $\mathrm{Li}(x)$ (at top of Section 3) by a *logarithmic integral function*. The constant $c = 1.038$ is a best fit to the numbers k. All endeavors to calculate c were fruitless; the combinatorial statistics of the n-sequences (in consequence of Theorem 3.2) got too complex: $c \approx 1$ is a random coincidence. Figure 1 and also Table 1 show that $T(b)$ is a good approximation to the counting number k.

It is well known that the density of prime natural numbers fluctuates. There are e.g. six primes p in the interval $97 \le p \le 113$, whereas, in $524 \le p \le 540$ of equal length, there is none. Similarly (see Table 1), there are seven q with five primes in the interval $2926 \le b \le 602\,056$, whereas, in the larger interval $602\,058 \le b \le 2\,071\,958$, there is none. Figure 1 shows that the fluctuations in sequences $S(b)$ with five primes are higher than in prime natural numbers.

It was shown that some GFN with fixed b have six primes. It can be expected that many more with six primes exist and that also more than six primes are possible.

Recently found: There exists a very similar set of *Generalized Fermat Numbers (GFN)* defined as $F_{b,n} = (b^{2^n} + 1)/2$ with $n \ge 0$ and b a positive *odd* integer. The first three elements of this set with at least *five primes* are $b = 3$ with $n = \{0, 1, 2, 4, 5, 6\}$ (even *six primes*), $b = 125\,001$ with $n = \{0, 1, 2, 4, 5\}$, and $b = 724\,741$ with $n = \{0, 1, 2, 4, 8\}$.

References

[1] T. M. Apostol, The fundamental theorem of arithmetic, in: *Introduction to analytic number theory*, Springer, Berlin (1976), 13–23.

[2] K. D. Boklan, J. H. Conway, Expect at most one billionth of a new Fermat prime, preprint (2016), arXiv:1605.01371v2.

[3] K. Chandrasekharan, *Introduction to analytic number theory*, Springer, Berlin, 1968.

[4] H. Dubner and Y. Gallot, Distribution of generalized Fermat prime numbers, *Math. Comp.* **71** (2002), 825–832.

[5] W. Narkiewicz, *The development of prime number theory*, Springer, Berlin, 2000.

[6] R. M. Robinson, Mersenne and Fermat numbers, *Proc. Amer. Math. Soc.* **5**, (1954), 842–846.

[7] T.-W. Sze, Deterministic primality proving on proth numbers, preprint (2008), arXiv:arXiv:0812.2596.

[8] t5k-Organisation *Record primes of this type*, https://t5k.org/top20/page.php?id=12 (2023), visited on 26 January 2024.

Gerold Brändli
Goldernstrasse 39
5000 Aarau, Switzerland
gerold.braendli@bluewin.ch

Jörg Waldvogel
Reutlenweg 27
8302 Kloten, Switzerland
waldvogel@math.ethz.ch