Wikipedia
The Free Encyclopedia

Fermat number

In mathematics, a **Fermat number**, named after Pierre de Fermat, who first studied them, is a positive integer of the form

$$F_n = 2^{2^n} + 1,$$

where n is a non-negative integer. The first few Fermat numbers are:

3, 5, 17, 257, 65537, 4294967297, 18446744073709551617, ... (sequence A000215 in the OEIS).

If $2^k + 1$ is prime and $k > 0$, then k must be a power of 2, so $2^k + 1$ is a Fermat number; such primes are called **Fermat primes**. As of 2023, the only known Fermat primes are $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, and $F_4 = 65537$ (sequence A019434 in the OEIS); heuristics suggest that there are no more.

Fermat prime

Named after	Pierre de Fermat
No. of known terms	5
Conjectured no. of terms	5
Subsequence of	Fermat numbers
First terms	3, 5, 17, 257, 65537
Largest known term	65537
OEIS index	A019434 (https://oeis.org/A019434)

Basic properties

The Fermat numbers satisfy the following recurrence relations:

$$F_n = (F_{n-1} - 1)^2 + 1$$

$$F_n = F_0 \cdots F_{n-1} + 2$$

for $n \geq 1$,

$$F_n = F_{n-1} + 2^{2^{n-1}} F_0 \cdots F_{n-2}$$

$$F_n = F_{n-1}^2 - 2(F_{n-2} - 1)^2$$

for $n \geq 2$. Each of these relations can be proved by mathematical induction. From the second equation, we can deduce **Goldbach's theorem** (named after Christian Goldbach): no two Fermat numbers share a common integer factor greater than 1. To see this, suppose that $0 \leq i < j$ and F_i and F_j have a common factor $a > 1$. Then a divides both

$$F_0 \cdots F_{j-1}$$

and F_j; hence a divides their difference, 2. Since $a > 1$, this forces $a = 2$. This is a contradiction, because each Fermat number is clearly odd. As a corollary, we obtain another proof of the infinitude of the prime numbers: for each F_n, choose a prime factor p_n; then the sequence $\{p_n\}$ is an infinite sequence of distinct primes.

Further properties

- No Fermat prime can be expressed as the difference of two pth powers, where p is an odd prime.
- With the exception of F_0 and F_1, the last digit of a Fermat number is 7.
- The sum of the reciprocals of all the Fermat numbers (sequence A051158 in the OEIS) is irrational. (Solomon W. Golomb, 1963)

Primality

Fermat numbers and Fermat primes were first studied by Pierre de Fermat, who conjectured that all Fermat numbers are prime. Indeed, the first five Fermat numbers $F_0, ..., F_4$ are easily shown to be prime. Fermat's conjecture was refuted by Leonhard Euler in 1732 when he showed that

$$F_5 = 2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \times 6700417.$$

Euler proved that every factor of F_n must have the form $k2^{n+1} + 1$ (later improved to $k2^{n+2} + 1$ by Lucas) for $n \geq 2$.

That 641 is a factor of F_5 can be deduced from the equalities $641 = 2^7 \times 5 + 1$ and $641 = 2^4 + 5^4$. It follows from the first equality that $2^7 \times 5 \equiv -1 \pmod{641}$ and therefore (raising to the fourth power) that $2^{28} \times 5^4 \equiv 1 \pmod{641}$. On the other hand, the second equality implies that $5^4 \equiv -2^4 \pmod{641}$. These congruences imply that $2^{32} \equiv -1 \pmod{641}$.

Fermat was probably aware of the form of the factors later proved by Euler, so it seems curious that he failed to follow through on the straightforward calculation to find the factor.[1] One common explanation is that Fermat made a computational mistake.

There are no other known Fermat primes F_n with $n > 4$, but little is known about Fermat numbers for large n.[2] In fact, each of the following is an open problem:

- Is F_n composite for all $n > 4$?
- Are there infinitely many Fermat primes? (Eisenstein 1844[3])
- Are there infinitely many composite Fermat numbers?
- Does a Fermat number exist that is not square-free?

As of 2014, it is known that F_n is composite for $5 \le n \le 32$, although of these, complete factorizations of F_n are known only for $0 \le n \le 11$, and there are no known prime factors for $n = 20$ and $n = 24$.[4] The largest Fermat number known to be composite is $F_{18233954}$, and its prime factor $7 \times 2^{18233956} + 1$ was discovered in October 2020.

Heuristic arguments

Heuristics suggest that F_4 is the last Fermat prime.

The prime number theorem implies that a random integer in a suitable interval around N is prime with probability $1/\ln N$. If one uses the heuristic that a Fermat number is prime with the same probability as a random integer of its size, and that F_5, ..., F_{32} are composite, then the expected number of Fermat primes beyond F_4 (or equivalently, beyond F_{32}) should be

$$\sum_{n\geq 33} \frac{1}{\ln F_n} < \frac{1}{\ln 2} \sum_{n\geq 33} \frac{1}{\log_2 (2^{2^n})} = \frac{1}{\ln 2} 2^{-32} < 3.36 \times 10^{-10}.$$

One may interpret this number as an upper bound for the probability that a Fermat prime beyond F_4 exists.

This argument is not a rigorous proof. For one thing, it assumes that Fermat numbers behave "randomly", but the factors of Fermat numbers have special properties. Boklan and Conway published a more precise analysis suggesting that the probability that there is another Fermat prime is less than one in a billion.[5]

Equivalent conditions

Let $F_n = 2^{2^n} + 1$ be the nth Fermat number. Pépin's test states that for $n > 0$,

> F_n is prime if and only if $3^{(F_n-1)/2} \equiv -1 \pmod{F_n}$.

The expression $3^{(F_n-1)/2}$ can be evaluated modulo F_n by repeated squaring. This makes the test a fast polynomial-time algorithm. But Fermat numbers grow so rapidly that only a handful of them can be tested in a reasonable amount of time and space.

There are some tests for numbers of the form $k2^m + 1$, such as factors of Fermat numbers, for primality.

> **Proth's theorem** (1878). Let $N = k2^m + 1$ with odd $k < 2^m$. If there is an integer a such that
>
> $$a^{(N-1)/2} \equiv -1 \pmod{N}$$
>
> then N is prime. Conversely, if the above congruence does not hold, and in addition
>
> $$\left(\frac{a}{N}\right) = -1$$ (See Jacobi symbol)
>
> then N is composite.

If $N = F_n > 3$, then the above Jacobi symbol is always equal to −1 for $a = 3$, and this special case of Proth's theorem is known as Pépin's test. Although Pépin's test and Proth's theorem have been implemented on computers to prove the compositeness of some Fermat numbers, neither test gives a specific nontrivial factor. In fact, no specific prime factors are known for $n = 20$ and 24.

Factorization

Because of Fermat numbers' size, it is difficult to factorize or even to check primality. Pépin's test gives a necessary and sufficient condition for primality of Fermat numbers, and can be implemented by modern computers. The elliptic curve method is a fast method for finding small prime divisors of numbers. Distributed computing project *Fermatsearch* has found some factors of Fermat numbers. Yves Gallot's proth.exe has been used to find factors of large Fermat numbers. Édouard Lucas, improving Euler's above-mentioned result, proved in 1878 that every factor of the Fermat number F_n, with n at least 2, is of the form $k \times 2^{n+2} + 1$ (see Proth number), where k is a positive integer. By itself, this makes it easy to prove the primality of the known Fermat primes.

Factorizations of the first twelve Fermat numbers are:

$F_0 = 2^1 + 1 = 3$ is prime
$F_1 = 2^2 + 1 = 5$ is prime
$F_2 = 2^4 + 1 = 17$ is prime
$F_3 = 2^8 + 1 = 257$ is prime
$F_4 = 2^{16} + 1 = 65{,}537$ is the largest known Fermat prime
$F_5 = 2^{32} + 1 = 4{,}294{,}967{,}297$
= 641 × 6,700,417 (fully factored 1732[6])
$F_6 = 2^{64} + 1$ = 18,446,744,073,709,551,617 (20 digits)
= 274,177 × 67,280,421,310,721 (14 digits) (fully factored 1855)
$F_7 = 2^{128} + 1$ = 340,282,366,920,938,463,463,374,607,431,768,211,457 (39 digits)
= 59,649,589,127,497,217 (17 digits) × 5,704,689,200,685,129,054,721 (22 digits) (fully factored 1970)
$F_8 = 2^{256} + 1$ = 115,792,089,237,316,195,423,570,985,008,687,907,853,269,984,665,640,564,039,457,584,007,913,129,639,937 (78 digits)
= 1,238,926,361,552,897 (16 digits) × 93,461,639,715,357,977,769,163,558,199,606,896,584,051,237,541,638,188,580,280,321 (62 digits) (fully factored 1980)
$F_9 = 2^{512} + 1$ = 13,407,807,929,942,597,099,574,024,998,205,846,127,479,365,820,592,393,377,723,561,443,721,764,030,073,546,976,801,874,298,166,903,427,690,031,858,186,486,050,853,753,882,811,946,569,946,433,649,006,084,097 (155 digits)
= 2,424,833 × 7,455,602,825,647,884,208,337,395,736,200,454,918,783,366,342,657 (49 digits) × 741,640,062,627,530,801,524,787,141,901,937,474,059,940,781,097,519,023,905,821,316,144,415,759,504,705,008,092,818,711,693,940,737 (99 digits) (fully factored 1990)
$F_{10} = 2^{1024} + 1$ = 179,769,313,486,231,590,772,930...304,835,356,329,624,224,137,217 (309 digits)
= 45,592,577 × 6,487,031,809 × 4,659,775,785,220,018,543,264,560,743,076,778,192,897 (40 digits) × 130,439,874,405,488,189,727,484...806,217,820,753,127,014,424,577 (252 digits) (fully factored 1995)
$F_{11} = 2^{2048} + 1$ = 32,317,006,071,311,007,300,714,8...193,555,853,611,059,596,230,657 (617 digits)
= 319,489 × 974,849 × 167,988,556,341,760,475,137 (21 digits) × 3,560,841,906,445,833,920,513 (22 digits) × 173,462,447,179,147,555,430,258...491,382,441,723,306,598,834,177 (564 digits) (fully factored 1988)

As of November 2021, only F_0 to F_{11} have been completely factored.[4] The distributed computing project Fermat Search is searching for new factors of Fermat numbers.[7] The set of all Fermat factors is A050922 (or, sorted, A023394) in OEIS.

The following factors of Fermat numbers were known before 1950 (since then, digital computers have helped find more factors):

Year	Finder	Fermat number	Factor
1732	Euler	F_5	$5 \cdot 2^7 + 1$
1732	Euler	F_5 (fully factored)	$52347 \cdot 2^7 + 1$
1855	Clausen	F_6	$1071 \cdot 2^8 + 1$
1855	Clausen	F_6 (fully factored)	$262814145745 \cdot 2^8 + 1$
1877	Pervushin	F_{12}	$7 \cdot 2^{14} + 1$
1878	Pervushin	F_{23}	$5 \cdot 2^{25} + 1$
1886	Seelhoff	F_{36}	$5 \cdot 2^{39} + 1$
1899	Cunningham	F_{11}	$39 \cdot 2^{13} + 1$
1899	Cunningham	F_{11}	$119 \cdot 2^{13} + 1$
1903	Western	F_9	$37 \cdot 2^{16} + 1$
1903	Western	F_{12}	$397 \cdot 2^{16} + 1$
1903	Western	F_{12}	$973 \cdot 2^{16} + 1$
1903	Western	F_{18}	$13 \cdot 2^{20} + 1$
1903	Cullen	F_{38}	$3 \cdot 2^{41} + 1$
1906	Morehead	F_{73}	$5 \cdot 2^{75} + 1$
1925	Kraitchik	F_{15}	$579 \cdot 2^{21} + 1$

As of January 2021, 356 prime factors of Fermat numbers are known, and 312 Fermat numbers are known to be composite.[4] Several new Fermat factors are found each year.[8]

Pseudoprimes and Fermat numbers

Like composite numbers of the form $2^p - 1$, every composite Fermat number is a strong pseudoprime to base 2. This is because all strong pseudoprimes to base 2 are also Fermat pseudoprimes – i.e.,

$$2^{F_n-1} \equiv 1 \pmod{F_n}$$

for all Fermat numbers.

In 1904, Cipolla showed that the product of at least two distinct prime or composite Fermat numbers $F_a F_b \dots F_s$, $a > b > \dots > s > 1$ will be a Fermat pseudoprime to base 2 if and only if $2^s > a$.[9]

Other theorems about Fermat numbers

Lemma. — If n is a positive integer,

$$a^n - b^n = (a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k}.$$

Proof

$$\begin{aligned}(a-b)\sum_{k=0}^{n-1} a^k b^{n-1-k} &= \sum_{k=0}^{n-1} a^{k+1} b^{n-1-k} - \sum_{k=0}^{n-1} a^k b^{n-k} \\ &= a^n + \sum_{k=1}^{n-1} a^k b^{n-k} - \sum_{k=1}^{n-1} a^k b^{n-k} - b^n \\ &= a^n - b^n\end{aligned}$$

Theorem — If $2^k + 1$ is an odd prime, then k is a power of 2.

Proof

If k is a positive integer but not a power of 2, it must have an odd prime factor $s > 2$, and we may write $k = rs$ where $1 \le r < k$.

By the preceding lemma, for positive integer m,

$$(a-b) \mid (a^m - b^m)$$

where $\mid$ means "evenly divides". Substituting $a = 2^r, b = -1$, and $m = s$ and using that s is odd,

$$(2^r + 1) \mid (2^{rs} + 1),$$

and thus

$$(2^r + 1) \mid (2^k + 1).$$

Because $1 < 2^r + 1 < 2^k + 1$, it follows that $2^k + 1$ is not prime. Therefore, by contraposition k must be a power of 2.

Theorem — A Fermat prime cannot be a Wieferich prime.

Proof

We show if $p = 2^m + 1$ is a Fermat prime (and hence by the above, m is a power of 2), then the congruence $2^{p-1} \equiv 1 \bmod p^2$ does not hold.

Since $2m|p-1$ we may write $p - 1 = 2m\lambda$. If the given congruence holds, then $p^2|2^{2m\lambda} - 1$, and therefore

$$0 \equiv \frac{2^{2m\lambda} - 1}{2^m + 1} = (2^m - 1)\left(1 + 2^{2m} + 2^{4m} + \cdots + 2^{2(\lambda-1)m}\right) \equiv -2\lambda \pmod{2^m + 1}.$$

Hence $2^m + 1|2\lambda$, and therefore $2\lambda \geq 2^m + 1$. This leads to $p - 1 \geq m(2^m + 1)$, which is impossible since $m \geq 2$.

Theorem (Édouard Lucas) — Any prime divisor p of $F_n = 2^{2^n} + 1$ is of the form $k2^{n+2} + 1$ whenever $n > 1$.

Sketch of proof

Let G_p denote the group of non-zero integers modulo p under multiplication, which has order $p - 1$. Notice that 2 (strictly speaking, its image modulo p) has multiplicative order equal to 2^{n+1} in G_p (since $2^{2^{n+1}}$ is the square of 2^{2^n} which is −1 modulo F_n), so that, by Lagrange's theorem, $p - 1$ is divisible by 2^{n+1} and p has the form $k2^{n+1} + 1$ for some integer k, as Euler knew. Édouard Lucas went further. Since $n > 1$, the prime p above is congruent to 1 modulo 8. Hence (as was known to Carl Friedrich Gauss), 2 is a quadratic residue modulo p, that is, there is integer a such that $p|a^2 - 2.$ Then the image of a has order 2^{n+2} in the group G_p and (using Lagrange's theorem again), $p - 1$ is divisible by 2^{n+2} and p has the form $s2^{n+2} + 1$ for some integer s.

In fact, it can be seen directly that 2 is a quadratic residue modulo p, since

$$\left(1 + 2^{2^{n-1}}\right)^2 \equiv 2^{1+2^{n-1}} \pmod{p}.$$

Since an odd power of 2 is a quadratic residue modulo p, so is 2 itself.

A Fermat number cannot be a perfect number or part of a pair of amicable numbers. (Luca 2000)

The series of reciprocals of all prime divisors of Fermat numbers is convergent. (Křížek, Luca & Somer 2002)

If $n^n + 1$ is prime, there exists an integer m such that $n = 2^{2^m}$. The equation $n^n + 1 = F_{(2^m+m)}$ holds in that case.[10][11]

Let the largest prime factor of the Fermat number F_n be $P(F_n)$. Then,

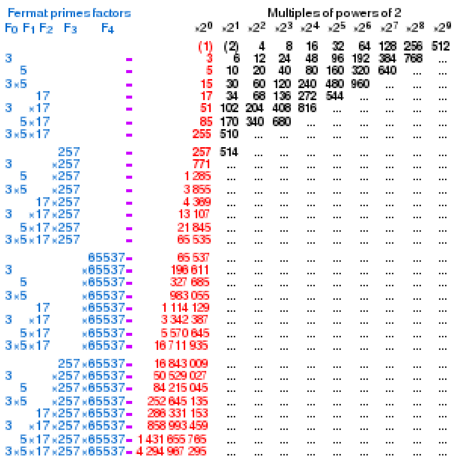
$P(F_n) \geq 2^{n+2}(4n + 9) + 1.$ (Grytczuk, Luca & Wójtowicz 2001)

Relationship to constructible polygons

Carl Friedrich Gauss developed the theory of Gaussian periods in his *Disquisitiones Arithmeticae* and formulated a sufficient condition for the constructibility of regular polygons. Gauss stated that this condition was also necessary,[12] but never published a proof. Pierre Wantzel gave a full proof of necessity in 1837. The result is known as the **Gauss–Wantzel theorem**:

> An n-sided regular polygon can be constructed with compass and straightedge if and only if n is the product of a power of 2 and distinct Fermat primes: in other words, if and only if n is of the form $n = 2^k p_1 p_2 \dots p_s$, where k, s are nonnegative integers and the p_i are distinct Fermat primes.

A positive integer n is of the above form if and only if its totient $\varphi(n)$ is a power of 2.



Number of sides of known constructible polygons having up to 1000 sides (bold) or odd side count (red)

Applications of Fermat numbers

Pseudorandom number generation

Fermat primes are particularly useful in generating pseudo-random sequences of numbers in the range 1, ..., N, where N is a power of 2. The most common method used is to take any seed value between 1 and $P - 1$, where P is a Fermat prime. Now multiply this by a number A, which is greater than the square root of P and is a primitive root modulo P (i.e., it is not a quadratic residue). Then take the result modulo P. The result is the new value for the RNG.

$$V_{j+1} = (A \times V_j) \bmod P$$ (see linear congruential generator, RANDU)

This is useful in computer science, since most data structures have members with 2^X possible values. For example, a byte has 256 (2^8) possible values (0–255). Therefore, to fill a byte or bytes with random values, a random number generator that produces values 1–256 can be used, the byte taking the output value −1. Very large Fermat primes are of particular interest in data encryption for this reason. This method produces only pseudorandom values, as after $P - 1$ repetitions, the sequence repeats. A poorly chosen multiplier can result in the sequence repeating sooner than $P - 1$.

Generalized Fermat numbers

Numbers of the form $a^{2^n} + b^{2^n}$ with a, b any coprime integers, $a > b > 0$, are called **generalized Fermat numbers**. An odd prime p is a generalized Fermat number if and only if p is congruent to 1 (mod 4). (Here we consider only the case $n > 0$, so $3 = 2^{2^0} + 1$ is not a counterexample.)

An example of a probable prime of this form is $1215^{131072} + 242^{131072}$ (found by Kellen Shenton).[13]

By analogy with the ordinary Fermat numbers, it is common to write generalized Fermat numbers of the form $a^{2^n} + 1$ as $F_n(a)$. In this notation, for instance, the number 100,000,001 would be written as $F_3(10)$. In the following we shall restrict ourselves to primes of this form, $a^{2^n} + 1$, such primes are called "Fermat primes base a". Of course, these primes exist only if a is even.

If we require $n > 0$, then Landau's fourth problem asks if there are infinitely many generalized Fermat primes $F_n(a)$.

Generalized Fermat primes

Because of the ease of proving their primality, generalized Fermat primes have become in recent years a topic for research within the field of number theory. Many of the largest known primes today are generalized Fermat primes.

Generalized Fermat numbers can be prime only for even a, because if a is odd then every generalized Fermat number will be divisible by 2. The smallest prime number $F_n(a)$ with $n > 4$ is $F_5(30)$, or $30^{32} + 1$. Besides, we can define "half generalized Fermat numbers" for an odd base, a half generalized Fermat number to base a (for odd a) is $\frac{a^{2^n} + 1}{2}$, and it is also to be expected that there will be only finitely many half generalized Fermat primes for each odd base.

(In the list, the generalized Fermat numbers ($F_n(a)$) to an even a are $a^{2^n} + 1$, for odd a, they are $\frac{a^{2^n}+1}{2}$. If a is a perfect power with an odd exponent (sequence A070265 in the OEIS), then all generalized Fermat number can be algebraic factored, so they cannot be prime)

(For the smallest number n such that $F_n(a)$ is prime, see OEIS: A253242)

a	numbers n such that $F_n(a)$ is prime	a	numbers n such that $F_n(a)$ is prime	a	numbers n such that $F_n(a)$ is prime	a	numbers n such that $F_n(a)$ is prime
2	0, 1, 2, 3, 4, …	18	0, …	34	2, …	50	…
3	0, 1, 2, 4, 5, 6, …	19	1, …	35	1, 2, 6, …	51	1, 3, 6, …
4	0, 1, 2, 3, …	20	1, 2, …	36	0, 1, …	52	0, …
5	0, 1, 2, …	21	0, 2, 5, …	37	0, …	53	3, …
6	0, 1, 2, …	22	0, …	38	…	54	1, 2, 5, …
7	2, …	23	2, …	39	1, 2, …	55	…
8	(none)	24	1, 2, …	40	0, 1, …	56	1, 2, …
9	0, 1, 3, 4, 5, …	25	0, 1, …	41	4, …	57	0, 2, …
10	0, 1, …	26	1, …	42	0, …	58	0, …
11	1, 2, …	27	(none)	43	3, …	59	1, …
12	0, …	28	0, 2, …	44	4, …	60	0, …
13	0, 2, 3, …	29	1, 2, 4, …	45	0, 1, …	61	0, 1, 2, …
14	1, …	30	0, 5, …	46	0, 2, 9, …	62	…
15	1, …	31	…	47	3, …	63	…
16	0, 1, 2, …	32	(none)	48	2, …	64	(none)
17	2, …	33	0, 3, …	49	1, …	65	1, 2, 5, …

b	known generalized (half) Fermat prime base *b*
2	3, 5, 17, 257, 65537
3	2, 5, 41, 21523361, 926510094425921, 1716841910146256242328924544641
4	5, 17, 257, 65537
5	3, 13, 313
6	7, 37, 1297
7	1201
8	(not possible)
9	5, 41, 21523361, 926510094425921, 1716841910146256242328924544641
10	11, 101
11	61, 7321
12	13
13	7, 14281, 407865361
14	197
15	113
16	17, 257, 65537
17	41761
18	19
19	181
20	401, 160001
21	11, 97241, 1023263388750334684164671319051311082339521
22	23
23	139921
24	577, 331777
25	13, 313
26	677
27	(not possible)
28	29, 614657
29	421, 353641, 125123236840173674393761
30	31, 18530201888518410000000000000000000000000000000001
31	
32	(not possible)
33	17, 703204309121
34	1336337
35	613, 750313, 330616742651687834074918381127337110499579842147487712949050636668246738736343104392290115356445313
36	37, 1297
37	19
38	
39	761, 1156721
40	41, 1601
41	31879515457326527173216321
42	43
43	5844100138801
44	197352587024076973231046657
45	23, 1013
46	47, 4477457, $46^{512}+1$ (852 digits: 214787904487…289480994817)
47	11905643330881
48	5308417
49	1201

50	

(See [14][15] for more information (even bases up to 1000), also see [16] for odd bases)

(For the smallest prime of the form $F_n(a, b)$ (for odd $a + b$), see also OEIS: A111635)

a	b	numbers n such that $\frac{a^{2^n}+b^{2^n}}{\gcd(a+b,2)} (= F_n(a,b))$ is prime
2	1	0, 1, 2, 3, 4, ...
3	1	0, 1, 2, 4, 5, 6, ...
3	2	0, 1, 2, ...
4	1	0, 1, 2, 3, ...
4	3	0, 2, 4, ...
5	1	0, 1, 2, ...
5	2	0, 1, 2, ...
5	3	1, 2, 3, ...
5	4	1, 2, ...
6	1	0, 1, 2, ...
6	5	0, 1, 3, 4, ...
7	1	2, ...
7	2	1, 2, ...
7	3	0, 1, 8, ...
7	4	0, 2, ...
7	5	1, 4, ...
7	6	0, 2, 4, ...
8	1	(none)
8	3	0, 1, 2, ...
8	5	0, 1, 2, ...
8	7	1, 4, ...
9	1	0, 1, 3, 4, 5, ...
9	2	0, 2, ...
9	4	0, 1, ...
9	5	0, 1, 2, ...
9	7	2, ...
9	8	0, 2, 5, ...
10	1	0, 1, ...
10	3	0, 1, 3, ...
10	7	0, 1, 2, ...
10	9	0, 1, 2, ...
11	1	1, 2, ...
11	2	0, 2, ...
11	3	0, 3, ...
11	4	1, 2, ...
11	5	1, ...
11	6	0, 1, 2, ...
11	7	2, 4, 5, ...
11	8	0, 6, ...
11	9	1, 2, ...
11	10	5, ...
12	1	0, ...
12	5	0, 4, ...
12	7	0, 1, 3, ...
12	11	0, ...
13	1	0, 2, 3, ...

13	2	1, 3, 9, …
13	3	1, 2, …
13	4	0, 2, …
13	5	1, 2, 4, …
13	6	0, 6, …
13	7	1, …
13	8	1, 3, 4, …
13	9	0, 3, …
13	10	0, 1, 2, 4, …
13	11	2, …
13	12	1, 2, 5, …
14	1	1, …
14	3	0, 3, …
14	5	0, 2, 4, 8, …
14	9	0, 1, 8, …
14	11	1, …
14	13	2, …
15	1	1, …
15	2	0, 1, …
15	4	0, 1, …
15	7	0, 1, 2, …
15	8	0, 2, 3, …
15	11	0, 1, 2, …
15	13	1, 4, …
15	14	0, 1, 2, 4, …
16	1	0, 1, 2, …
16	3	0, 2, 8, …
16	5	1, 2, …
16	7	0, 6, …
16	9	1, 3, …
16	11	2, 4, …
16	13	0, 3, …
16	15	0, …

(For the smallest even base a such that $F_n(a)$ is prime, see OEIS: A056993)

n	bases a such that $F_n(a)$ is prime (only consider even a)	OEIS sequence
0	2, 4, 6, 10, 12, 16, 18, 22, 28, 30, 36, 40, 42, 46, 52, 58, 60, 66, 70, 72, 78, 82, 88, 96, 100, 102, 106, 108, 112, 126, 130, 136, 138, 148, 150, …	A006093
1	2, 4, 6, 10, 14, 16, 20, 24, 26, 36, 40, 54, 56, 66, 74, 84, 90, 94, 110, 116, 120, 124, 126, 130, 134, 146, 150, 156, 160, 170, 176, 180, 184, …	A005574
2	2, 4, 6, 16, 20, 24, 28, 34, 46, 48, 54, 56, 74, 80, 82, 88, 90, 106, 118, 132, 140, 142, 154, 160, 164, 174, 180, 194, 198, 204, 210, 220, 228, …	A000068
3	2, 4, 118, 132, 140, 152, 208, 240, 242, 288, 290, 306, 378, 392, 426, 434, 442, 508, 510, 540, 542, 562, 596, 610, 664, 680, 682, 732, 782, …	A006314
4	2, 44, 74, 76, 94, 156, 158, 176, 188, 198, 248, 288, 306, 318, 330, 348, 370, 382, 396, 452, 456, 470, 474, 476, 478, 560, 568, 598, 642, …	A006313
5	30, 54, 96, 112, 114, 132, 156, 332, 342, 360, 376, 428, 430, 432, 448, 562, 588, 726, 738, 804, 850, 884, 1068, 1142, 1198, 1306, 1540, 1568, …	A006315
6	102, 162, 274, 300, 412, 562, 592, 728, 1084, 1094, 1108, 1120, 1200, 1558, 1566, 1630, 1804, 1876, 2094, 2162, 2164, 2238, 2336, 2388, …	A006316
7	120, 190, 234, 506, 532, 548, 960, 1738, 1786, 2884, 3000, 3420, 3476, 3658, 4258, 5788, 6080, 6562, 6750, 7692, 8296, 9108, 9356, 9582, …	A056994
8	278, 614, 892, 898, 1348, 1494, 1574, 1938, 2116, 2122, 2278, 2762, 3434, 4094, 4204, 4728, 5712, 5744, 6066, 6508, 6930, 7022, 7332, …	A056995
9	46, 1036, 1318, 1342, 2472, 2926, 3154, 3878, 4386, 4464, 4474, 4482, 4616, 4688, 5374, 5698, 5716, 5770, 6268, 6386, 6682, 7388, 7992, …	A057465
10	824, 1476, 1632, 2462, 2484, 2520, 3064, 3402, 3820, 4026, 6640, 7026, 7158, 9070, 12202, 12548, 12994, 13042, 15358, 17646, 17670, …	A057002
11	150, 2558, 4650, 4772, 11272, 13236, 15048, 23302, 26946, 29504, 31614, 33308, 35054, 36702, 37062, 39020, 39056, 43738, 44174, 45654, …	A088361
12	1534, 7316, 17582, 18224, 28234, 34954, 41336, 48824, 51558, 51914, 57394, 61686, 62060, 89762, 96632, 98242, 100540, 101578, 109696, …	A088362
13	30406, 71852, 85654, 111850, 126308, 134492, 144642, 147942, 150152, 165894, 176206, 180924, 201170, 212724, 222764, 225174, 241600, …	A226528
14	67234, 101830, 114024, 133858, 162192, 165306, 210714, 216968, 229310, 232798, 422666, 426690, 449732, 462470, 468144, 498904, 506664, …	A226529
15	70906, 167176, 204462, 249830, 321164, 330716, 332554, 429370, 499310, 524552, 553602, 743788, 825324, 831648, 855124, 999236, 1041870, …	A226530
16	48594, 108368, 141146, 189590, 255694, 291726, 292550, 357868, 440846, 544118, 549868, 671600, 843832, 857678, 1024390, 1057476, 1087540, …	A251597
17	62722, 130816, 228188, 386892, 572186, 689186, 909548, 1063730, 1176694, 1361244, 1372930, 1560730, 1660830, 1717162, 1722230, 1766192, …	A253854
18	24518, 40734, 145310, 361658, 525094, 676754, 773620, 1415198, 1488256, 1615588, 1828858, 2042774, 2514168, 2611294, 2676404, 3060772, …	A244150
19	75898, 341112, 356926, 475856, 1880370, 2061748, 2312092, 2733014, 2788032, 2877652, 2985036, 3214654, 3638450, 4896418, 5897794, …	A243959
20	919444, 1059094, 1951734, 1963736, …	A321323

The smallest base b such that $b^{2^n} + 1$ is prime are

2, 2, 2, 2, 2, 30, 102, 120, 278, 46, 824, 150, 1534, 30406, 67234, 70906, 48594, 62722, 24518, 75898, 919444, ... (sequence A056993 in the OEIS)

The smallest k such that $(2n)^k + 1$ is prime are

1, 1, 1, 0, 1, 1, 2, 1, 1, 2, 1, 2, 2, 1, 1, 0, 4, 1, ... (The next term is unknown) (sequence A079706 in the OEIS) (also see OEIS: A228101 and OEIS: A084712)

A more elaborate theory can be used to predict the number of bases for which $F_n(a)$ will be prime for fixed n. The number of generalized Fermat primes can be roughly expected to halve as n is increased by 1.

Largest known generalized Fermat primes

The following is a list of the 5 largest known generalized Fermat primes.[17] The whole top-5 is discovered by participants in the PrimeGrid project.

Rank	Prime number	Generalized Fermat notation	Number of digits	Discovery date	ref.
1	$1963736^{1048576} + 1$	$F_{20}(1963736)$	6,598,776	Sep 2022	[18]
2	$1951734^{1048576} + 1$	$F_{20}(1951734)$	6,595,985	Aug 2022	[19]
3	$1059094^{1048576} + 1$	$F_{20}(1059094)$	6,317,602	Nov 2018	[20]
4	$919444^{1048576} + 1$	$F_{20}(919444)$	6,253,210	Sep 2017	[21]
5	$25 \times 2^{13719266} + 1$	$F_1(5 \times 2^{6859633})$	4,129,912	Sep 2022	[22]

On the Prime Pages one can find the current top 100 generalized Fermat primes (http://primes.utm.edu/primes/search.php?Comment=Generalized+Fermat&OnList=yes&Number=100&Style=HTML).

See also

- Constructible polygon: which regular polygons are constructible partially depends on Fermat primes.
- Double exponential function
- Lucas' theorem
- Mersenne prime
- Pierpont prime
- Primality test
- Proth's theorem
- Pseudoprime
- Sierpiński number
- Sylvester's sequence

Notes

1. Křížek, Luca & Somer 2001, p. 38, Remark 4.15
2. Chris Caldwell, "Prime Links++: special forms" (http://primes.utm.edu/links/theory/special_forms/) Archived (https://web.archive.org/web/20131224224552/http://primes.utm.edu/links/theory/special_forms/) 2013-12-24 at the Wayback Machine at The Prime Pages.
3. Ribenboim 1996, p. 88.
4. Keller, Wilfrid (January 18, 2021), "Prime Factors of Fermat Numbers" (http://www.prothsearch.com/fermat.html#Summary), *ProthSearch.com*, retrieved January 19, 2021
5. Boklan, Kent D.; Conway, John H. (2017). "Expect at most one billionth of a new Fermat Prime!". *The Mathematical Intelligencer*. **39** (1): 3–5. arXiv:1605.01371 (https://arxiv.org/abs/1605.01371). doi:10.1007/s00283-016-9644-3 (https://doi.org/10.1007%2Fs00283-016-9644-3). S2CID 119165671 (https://api.semanticscholar.org/CorpusID:119165671).
6. Sandifer, Ed. "How Euler Did it" (http://eulerarchive.maa.org/hedi/HEDI-2007-03.pdf) (PDF). *MAA Online*. Mathematical Association of America. Archived (https://ghostarchive.org/archive/20221009/http://eulerarchive.maa.org/hedi/HEDI-2007-03.pdf) (PDF) from the original on 2022-10-09. Retrieved 2020-06-13.
7. ":: F E R M A T S E A R C H . O R G :: Home page" (http://www.fermatsearch.org/). *www.fermatsearch.org*. Retrieved 7 April 2018.
8. "::FERMATSEARCH.ORG:: News" (http://www.fermatsearch.org/news.html). *www.fermatsearch.org*. Retrieved 7 April 2018.
9. Krizek, Michal; Luca, Florian; Somer, Lawrence (14 March 2013). *17 Lectures on Fermat Numbers: From Number Theory to Geometry* (https://books.google.com/books?id=hgfSBwAAQBAJ&q=cipolla+fermat+1904&pg=PA132). Springer Science & Business Media. ISBN 9780387218502. Retrieved 7 April 2018 – via Google Books.
10. Jeppe Stig Nielsen, "S(n) = n^n + 1" (http://jeppesn.dk/nton.html).
11. Weisstein, Eric W. "Sierpiński Number of the First Kind" (https://mathworld.wolfram.com/SierpinskiNumberoftheFirstKind.html). *MathWorld*.
12. Gauss, Carl Friedrich (1966). *Disquisitiones arithmeticae* (https://archive.org/details/disquisitionesar0000carl/). New Haven and London: Yale University Press. pp. 458–460. Retrieved 25 January 2023.
13. PRP Top Records, search for x^131072+y^131072 (http://www.primenumbers.net/prptop/searchform.php?form=x%5E131072%2By%5E131072&action=Search), by Henri & Renaud Lifchitz.
14. "Generalized Fermat Primes" (http://jeppesn.dk/generalized-fermat.html). *jeppesn.dk*. Retrieved 7 April 2018.
15. "Generalized Fermat primes for bases up to 1030" (http://www.noprimeleftbehind.net/crus/GFN-primes.htm). *noprimeleftbehind.net*. Retrieved 7 April 2018.
16. "Generalized Fermat primes in odd bases" (http://www.fermatquotient.com/PrimSerien/GenFermOdd.txt). *fermatquotient.com*. Retrieved 7 April 2018.
17. Caldwell, Chris K. "The Top Twenty: Generalized Fermat" (http://primes.utm.edu/top20/page.php?id=12). *The Prime Pages*. Retrieved 11 July 2019.
18. $1963736^{1048576} + 1$ (https://primes.utm.edu/primes/page.php?id=134423)
19. $1951734^{1048576} + 1$ (https://primes.utm.edu/primes/page.php?id=134298)

20. $1059094^{1048576}+1$ (https://primes.utm.edu/primes/page.php?id=125753)
21. $919444^{1048576}+1$ (https://primes.utm.edu/primes/page.php?id=123875)
22. $25*2^{13719266}+1$ (https://primes.utm.edu/primes/page.php?id=134407)

References

- Golomb, S. W. (January 1, 1963), "On the sum of the reciprocals of the Fermat numbers and related irrationalities", *Canadian Journal of Mathematics*, **15**: 475–478, doi:10.4153/CJM-1963-051-0 (https://doi.org/10.4153%2FCJM-1963-051-0), S2CID 123138118 (https://api.semanticscholar.org/CorpusID:123138118)
- Grytczuk, A.; Luca, F. & Wójtowicz, M. (2001), "Another note on the greatest prime factors of Fermat numbers", *Southeast Asian Bulletin of Mathematics*, **25** (1): 111–115, doi:10.1007/s10012-001-0111-4 (https://doi.org/10.1007%2Fs10012-001-0111-4), S2CID 122332537 (https://api.semanticscholar.org/CorpusID:122332537)
- Guy, Richard K. (2004), *Unsolved Problems in Number Theory* (https://www.springer.com/mathematics/numbers/book/978-0-387-20860-2?otherVersion=978-0-387-26677-0), Problem Books in Mathematics, vol. 1 (3rd ed.), New York: Springer Verlag, pp. A3, A12, B21, ISBN 978-0-387-20860-2
- Křížek, Michal; Luca, Florian & Somer, Lawrence (2001), *17 Lectures on Fermat Numbers: From Number Theory to Geometry* (https://www.springer.com/mathematics/numbers/book/978-0-387-95332-8), CMS books in mathematics, vol. 10, New York: Springer, ISBN 978-0-387-95332-8 - This book contains an extensive list of references.
- Křížek, Michal; Luca, Florian & Somer, Lawrence (2002), "On the convergence of series of reciprocals of primes related to the Fermat numbers", *Journal of Number Theory*, **97** (1): 95–112, doi:10.1006/jnth.2002.2782 (https://doi.org/10.1006%2Fjnth.2002.2782)
- Luca, Florian (2000), "The anti-social Fermat number" (http://www.maa.org/publications/periodicals/american-mathematical-monthly/american-mathematical-monthly-february-2000), *American Mathematical Monthly*, **107** (2): 171–173, doi:10.2307/2589441 (https://doi.org/10.2307%2F2589441), JSTOR 2589441 (https://www.jstor.org/stable/2589441)
- Ribenboim, Paulo (1996), *The New Book of Prime Number Records* (https://www.springer.com/mathematics/numbers/book/978-0-387-94457-9) (3rd ed.), New York: Springer, ISBN 978-0-387-94457-9
- Robinson, Raphael M. (1954), "Mersenne and Fermat Numbers", *Proceedings of the American Mathematical Society*, **5** (5): 842–846, doi:10.2307/2031878 (https://doi.org/10.2307%2F2031878), JSTOR 2031878 (https://www.jstor.org/stable/2031878)
- Yabuta, M. (2001), "A simple proof of Carmichael's theorem on primitive divisors" (http://www.fq.math.ca/Scanned/39-5/yabuta.pdf) (PDF), *Fibonacci Quarterly*, **39**: 439–443, archived (https://ghostarchive.org/archive/20221009/http://www.fq.math.ca/Scanned/39-5/yabuta.pdf) (PDF) from the original on 2022-10-09

External links

- Chris Caldwell, The Prime Glossary: Fermat number (http://primes.utm.edu/glossary/page.php?sort=FermatNumber) at The Prime Pages.
- Luigi Morelli, History of Fermat Numbers (http://www.fermatsearch.org/history.html)
- John Cosgrave, Unification of Mersenne and Fermat Numbers (http://johnbcosgrave.com/archive/fermat6.htm)
- Wilfrid Keller, Prime Factors of Fermat Numbers (http://www.prothsearch.com/fermat.html)
- Weisstein, Eric W. "Fermat Number" (https://mathworld.wolfram.com/FermatNumber.html). *MathWorld*.
- Weisstein, Eric W. "Fermat Prime" (https://mathworld.wolfram.com/FermatPrime.html). *MathWorld*.
- Weisstein, Eric W. "Generalized Fermat Number" (https://mathworld.wolfram.com/GeneralizedFermatNumber.html). *MathWorld*.
- Yves Gallot, Generalized Fermat Prime Search (http://pagesperso-orange.fr/yves.gallot/primes/index.html)
- Mark S. Manasse, Complete factorization of the ninth Fermat number (https://groups.google.com/forum/#!topic/sci.math/7usZOcN2_zc) (original announcement)
- Peyton Hayslette, Largest Known Generalized Fermat Prime Announcement (http://www.primegrid.com/download/GFN-341112_524288.pdf)