Acta Mathematica et Informatica Universitatis Ostraviensis

Michal Křížek; Lawrence Somer

17 necessary and sufficient conditions for the primality of Fermat numbers

Acta Mathematica et Informatica Universitatis Ostraviensis, Vol. 11 (2003), No. 1, 73--79

Persistent URL: `http://dml.cz/dmlcz/120594`

17 necessary and sufficient conditions for the primality of Fermat numbers

Michal Křížek and Lawrence Somer

ABSTRACT. We give a survey of necessary and sufficient conditions on the primality of the Fermat number $F_m = 2^{2^m} + 1$. Some new connections with graph theory are presented.

1. Introduction

In 1640, Pierre de Fermat conjectured that all numbers

$$F_m = 2^{2^m} + 1 \quad \text{for } m = 0,\ 1,\ 2, \ldots, \tag{1}$$

are prime, which was later found to be incorrect. The numbers F_m are called *Fermat numbers* after him. If F_m is prime, we say that it is a *Fermat prime*.

Until the end of the 18th century, Fermat numbers were most likely a mathematical curiosity. The interest in the Fermat numbers dramatically increased when the German mathematician C. F. Gauss quite unexpectedly found (see [3, Sect. VII]) that there exists a Euclidean construction (by ruler and compass) of the regular polygon with n sides if

$$n = 2^i F_{m_1} F_{m_2} \cdots F_{m_j},$$

where $n \geq 3$, $i \geq 0$, $j \geq 0$, and $F_{m_1},\ F_{m_2}, \ldots,\ F_{m_j}$ are distinct Fermat primes (for $j = 0$ no Fermat primes appear in the above factorization of n). Gauss stated that the converse implication is true as well, but did not prove it. This was proved later in 1837 (see [17]).

At present we know that the first five members of sequence (1) are prime and that (see [2])

$$F_m \text{ is composite for } 5 \leq m \leq 32.$$

The compositeness of F_5 was found by Leonhard Euler in 1732. In 1855, Thomas Clausen gave the complete factorization of F_6 into two prime factors (see [1, p. 185],

2000 *Mathematics Subject Classification:* 11A07, 11A15, 11A51, 05C20.
Key words and phrases: Fermat numbers, primitive roots, primality, graph theory.

[7, p. 4]). In [12], it was shown that F_7 is composite. For a survey of the factorizations of further Fermat numbers, see, e.g., [7, Chapt. 1]. Note that the status of F_{33} is unknown at present.

In Theorems 1 – 3 below, we introduce three sets of necessary and sufficient conditions for Fermat primes. Most of them are proved in [7].

2. Necessary and sufficient conditions for an integer to be a Fermat prime

For an integer $n > 1$ define

$$M(n) = \{a \in \{1, ..., n-1\} \mid a \text{ is a primitive root} \pmod{n}\}$$

and

$$K(n) = \{a \in \{1, ..., n-1\} \mid \gcd(a, n) = 1 \text{ and } a \text{ is a quadratic nonresidue} \pmod{n}\}.$$

In Theorem 1 below, we shall see how the relation $M(n) = K(n)$ is connected with Fermat primes.

Further, let

$$H = \{0, 1, \ldots, n-1\}$$

and let f be a map of H into itself. The *iteration digraph* of f is a directed graph whose vertices are elements of H and such that there exists a directed edge from x to $f(x)$ for all $x \in H$. A *component* of the iteration digraph is a subdiagraph which is a maximal connected subgraph of the symmetrization of this digraph (i.e., the associated nondirected graph). The iteration digraph is called a *binary digraph* if it has exactly two components and the following three conditions hold:

1) the vertex 0 is an isolated fixed point,

2) the vertex 1 is a fixed point and there exists a directed edge from the vertex $n-1$ to 1,

3) for each vertex from the set $\{1, 2, \ldots, n-1\}$ there exist either two edges or no edge directed toward this vertex.

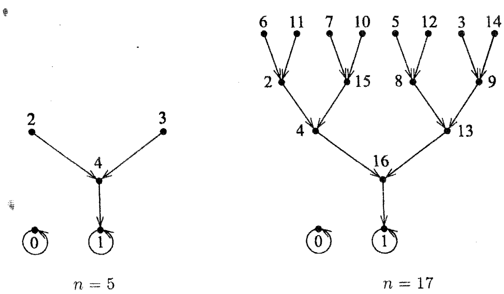

Fig. 1. Binary digraphs corresponding to Fermat primes.

We will consider a special discrete iteration. For each $x \in H$ let $f(x)$ be the remainder of x^2 modulo n, i.e.,

$$f(x) \in H \quad \text{and} \quad f(x) \equiv x^2 \pmod{n}. \tag{2}$$

This corresponds to the iteration scheme $x_{k+1} \equiv x_k^2 \pmod{n}$. In Theorem 1, we shall again see how this iteration scheme is connected with Fermat primes (cf. Figure 1).

From here on, whenever we refer to the iteration digraph of f, we always assume that the mapping f is as given in (2).

Furthermore, we describe a graphical procedure which transforms algebraic fractions $\frac{1}{n}$ to geometric images. Let $b > 1$ and n be positive integers. If r_i is the remainder produced at step i of the base b long division of $\frac{1}{n}$, then the remainder produced at the $(i+1)$st step obviously satisfies the congruence

$$r_{i+1} \equiv br_i \pmod{n}.$$

Starting with $r_0 = 1$, we get the sequence of remainders $r_0, r_1, r_2, \ldots$ of $\frac{1}{n}$ obtained through long division in base b. We may graphically analyze this fraction. This analysis begins at the point (r_0, r_0), proceeds first vertically, then horizontally to (r_1, r_1), then moves again vertically, then horizontally to (r_2, r_2), and continues in this fashion (compare with Figure 2). If the remainder becomes zero at the ith step, we stop the process. In this way, the sequence of remainders entirely determines the associated graph of the fraction.

Consider, for example, the fraction $\frac{1}{7}$, which has a base 10 (decimal) expansion of $0.\overline{142857}$. The corresponding sequence of remainders is periodic: $r_0 = 1$, $r_1 = 3 \equiv 10 \pmod{7}$, $r_2 = 2 \equiv 30 \pmod{7}$, $r_3 = 6 \equiv 20 \pmod{7}$, $r_4 = 4 \equiv 60 \pmod{7}$, $r_5 = 5 \equiv 40 \pmod{7}$, $r_0 = r_6 = 1 \equiv 50 \pmod{7}$, etc. In Figure 2, we see that the associated graph possesses a rotational symmetry with respect to the point $(3.5, 3.5)$ for the base $b = 10$, but the graph is nonsymmetric for $b = 11$. The graphical analysis of the fraction $\frac{1}{F_m}$ for $m = 2$ is illustrated in Figure 3.

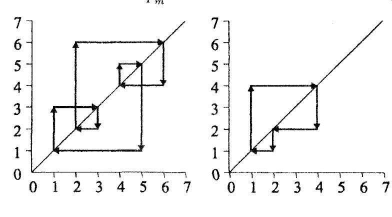

Fig. 2. Graphical analysis of $\frac{1}{7}$ for two different bases.

An integer $n > 1$ is said to be *perfectly symmetric* if the associated graph of its reciprocal $\frac{1}{n}$ is rotationally symmetric with respect to the point $\left(\frac{n}{2}, \frac{n}{2}\right)$ in any base b provided $b \not\equiv 0 \pmod{n}$ and $b \not\equiv 1 \pmod{n}$.

Theorem 1. *The integer n is a Fermat prime if and only if one of the following conditions holds:*

(i) The integer $n \geq 3$ is odd and $M(n) = K(n)$.

(ii) The iteration digraph of f is a binary digraph.

(iii) The integer $n \geq 3$ and the iteration digraph of f has exactly two components and zero is an isolated fixed point.

(iv) The integer $n \geq 3$ is odd and the iteration digraph of f has exactly two components.

(v) The integer $n \geq 3$ is perfectly symmetric.

The proof of (i) is given in [8]. For the proof of (ii), see [15]. The proofs of (iii) and (iv) follow from Theorems 2.1 and 4.4 from [14]. The proof of property (v) can be found in [5].

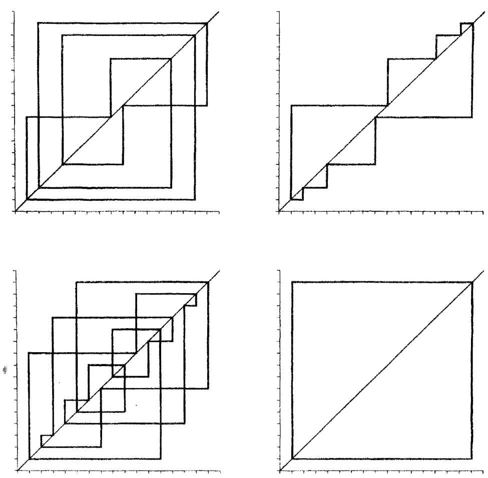

Fig. 3. Graphical analysis of $\frac{1}{17}$ for $b = 8,\ 9,\ 10$, and 16.

3. Necessary and sufficient conditions for the primality of Fermat numbers

Before we state further necessary and sufficient conditions for the primality of Fermat numbers, we recall a well-known property of the *Euler totient function* ϕ:

If the prime power factorization of n is given by

$$n = \prod_{i=1}^{r} p_i^{k_i},$$

where $p_1 < p_2 < \cdots < p_r$, $k_i > 0$, then

$$\phi(n) = \prod_{i=1}^{r} (p_i - 1)p_i^{k_i - 1}. \tag{3}$$

Theorem 2. *For $m \geq 1$, the Fermat number F_m is prime if and only if one of the following conditions holds:*

(vi) There exists a Euclidean construction of the regular polygon with F_m sides by ruler and compass.

(vii)

$$\phi(F_m) = 2^{2^m}.$$

(viii) There exists $n \geq 1$ such that $\phi(F_m) = 2^n$.

(ix)

$$3^{(F_m - 1)/2} \equiv -1 \pmod{F_m} \quad \textit{(Pepin's test)}.$$

(x) The number F_m divides the term R_{2^m-2} of the sequence defined by

$$R_0 = 8, \quad R_i = R_{i-1}^2 - 2, \quad i = 1,\ 2, \ldots\ .$$

(xi) The number F_m does not divide $T(F_m - 2)$, where $T(n)$ is defined by means of the power series

$$\tan z = \sum_{n=0}^{\infty} \frac{T(n)z^n}{n!}.$$

(xii) The number F_m can be written as a sum of two nonzero squares in essentially only one way, namely $F_m = \left(2^{2^{m-1}}\right)^2 + 1^2$.

(xiii) There exists a Heron triangle,[1] whose sides all have prime power lengths such that at least one of the lengths is equal to F_m.

(xiv) There does not exist a factor $k2^n + 1$ of F_m, where $k \geq 3$ is odd and $n \geq m + 2$.

(xv) $3h2^{m+2} + 1 \nmid F_m$ for any positive integer h.

P r o o f . (vi) This is a special case of the famous Gauss's theorem ([3], [7]).

(vii) The proof immediately follows from well-known properties of the Euler totient function (see (3)).

(viii) If F_m is prime then by (vii),

$$\phi(F_m) = 2^{2^m}.$$

Now assume by the way of contradiction that F_m is a composite number and that $\phi(F_m) = 2^n$ for some $n \geq 1$. Then there exists an odd prime $p < F_m$ such that $p \mid F_m$. Consequently, $p - 1 \mid \phi(F_m)$ by (3), and hence, $p - 1 = 2^c$ for some $c < n$.

[1] A *Heron triangle* is a triangle such that the lengths of its three sides as well as its area are integers.

Therefore, p is a Fermat prime, which is impossible due to Goldbach's theorem (see, e.g., [7, p. 33]), which says that any two different Fermat numbers are coprime.

(ix) For the proof see [7, p. 42] (the base 5 is treated in the original paper by Pepin [13]).

(x) For the proof see [4].

(xi) For the proof see [11].

(xii) This result is a special case of the so-called Fermat's assertion, which says that every prime of the form $4k+1$ can be written as a sum of two nonzero squares in exactly one way. For a detailed proof see, e.g., [7, p. 49].

(xiii) The proof can be found in [9].

(xiv) This result follows from the famous theorem due to Lucas [10].

(xv) The proof is an immediate consequence of the main theorem from the paper [6, p. 439]. □

In Theorem 3 we will restrict the form of the index m in F_m.

Theorem 3.

(xvi) Let m be a prime of the form $4k+3$ and $M_m = 2^m - 1$ be the associated Mersenne number. Then the Fermat number F_m is prime if and only if

$$M_m^{(F_m-1)/2} \equiv -1 \pmod{F_m}.$$

(xvii) Let m be a prime of the form $8k+3$ or $8k+5$ and $M_m = 2^m - 1$ be the associated Mersenne number. Then the Fermat number F_m is prime if and only if

$$M_m^{(F_{m+1}-1)/2} \equiv -1 \pmod{F_{m+1}}.$$

These necessary and sufficient conditions are proved in [16].

Although hundreds of factors of the Fermat numbers and many necessary and sufficient conditions for the primality of F_m are known, no one has been able to discover a general principle that would lead to a definitive answer to the question whether F_4 is the largest Fermat prime.

Acknowledgement. This paper was supported by grant No. 201/02/1057 of the Grant Agency of the Czech Republic.

References

[1] Biermann, K.-R. *Thomas Clausen, Mathematiker und Astronom* J. Reine Angew. Math. **216**, 1964, 159–198.

[2] Crandall, R. E., Mayer, E., Papadopoulos, J. *The twenty-fourth Fermat number is composite* Math. Comp., accepted, 1999, 1–21.

[3] Gauss, C. F. *Disquisitiones arithmeticae* Springer, Berlin1986

[4] Inkeri, K. *Tests for primality* Ann. Acad. Sci. Fenn. Ser. A I No. 279 1960, 1–19.

[5] Jones, R., Pearce, J. *A postmodern view of fractions and the reciprocals of Fermat primes* Math. Mag. **73**, 2000, 83–97.

[6] Křížek, M., Chleboun, J. *A note on factorization of the Fermat numbers and their factors of the form $3h2^n+1$* Math. Bohem. **119**, 1994, 437–445.

[7] Křížek, M., Luca, F., Somer, L. *17 lectures on the Fermat numbers. From number theory to geometry* Springer-Verlag, New York 2001

[8] Křížek, M., Somer, L. *A necessary and sufficient condition for the primality of Fermat numbers* Math. Bohem. **126**, 2001, 541–549.

[9] Luca, F. *Fermat numbers and Heron triangles with prime power sides* Amer. Math. Monthly, accepted in 2000

[10] Lucas, E. *Théorèmes d'arithmétique* Atti della Reale Accademia delle Scienze di Torino **13**, 1878, 271–284.

[11] McIntosh, R. *A necessary and sufficient condition for the primality of Fermat numbers* Amer. Math. Monthly **90**, 1983, 98–99.

[12] Morehead, J. C. *Note on Fermat's numbers* Bull. Amer. Math. Soc. **11**, 1905, 543–545.

[13] Pepin, P. *Sur la formule* $2^{2^n}+1$ C. R. Acad. Sci. **85**, 1877, 329–331.

[14] Somer, L., Křížek, M. *On a connection of number theory with graph theory* Czechoslovak Math. J. (submitted)

[15] Szalay, L. *A discrete iteration in number theory, (Hungarian)* BDTF Tud. Közl. VIII. Természettudományok 3., Szombathely, 1992, 71–91.

[16] Vasilenko, O. N. *On some properties of Fermat numbers, (Russian)* Vestnik Moskov. Univ. Ser. I Mat. Mekh., no. 5 1998, 56–58.

[17] Wantzel, P. L. *Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas* J. Math. **2**, 1837, 366–372.

Michal Křížek, Mathematical Institute, Academy of Sciences, Žitná 25, CZ – 115 67 Prague 1, Czech Republica

Lawrence Somer, Department of Mathematics, Catholic University of America, Washington, D.C. 20064, U.S.A.