A NECESSARY AND SUFFICIENT CONDITION FOR THE PRIMALITY OF FERMAT NUMBERS

Michal Křížek, Praha, Lawrence Somer, Washington

(Received July 14, 2000)

Abstract. We examine primitive roots modulo the Fermat number $F_m = 2^{2^m} + 1$. We show that an odd integer $n \geqslant 3$ is a Fermat prime if and only if the set of primitive roots modulo n is equal to the set of quadratic non-residues modulo n. This result is extended to primitive roots modulo twice a Fermat number.

Keywords: Fermat numbers, primitive roots, primality, Sophie Germain primes

MSC 2000: 11A07, 11A15, 11A51

1. Introduction

Pierre de Fermat conjectured that all numbers

$$F_m = 2^{2^m} + 1 \quad \text{for } m = 0, 1, 2, \ldots \tag{1.1}$$

are prime. Nowadays we know that the first five members of this sequence are prime and that (see [2])

$$F_m \text{ is composite for } 5 \leqslant m \leqslant 30. \tag{1.2}$$

The status of F_{31} is for the time being unknown, i.e., we do not know yet whether it is prime or composite.

The numbers F_m are called *Fermat numbers*. If F_m is prime, we say that it is a *Fermat prime*.

Until 1796 Fermat numbers were most likely a mathematical curiosity. The interest in the Fermat primes dramatically increased when C. F. Gauss stated that there is a remarkable connection between the Euclidean construction (i.e., by ruler and compass) of regular polygons and the Fermat numbers. In particular, he proved that if the number of sides of a regular polygon is of the form $2^k F_{m_1} \ldots F_{m_r}$, where $k \geqslant 0$, $r \geqslant 0$, and F_{m_i} are distinct Fermat primes, then this polygon can be constructed by ruler and compass. The converse statement was established later by Wantzel in [8].

There exist many necessary and sufficient conditions concerning the primality of F_m. For instance, the number F_m $(m > 0)$ is a prime if and only if it can be written as a sum of two squares in essentially only one way, namely $F_m = \left(2^{2^{m-1}}\right)^2 + 1^2$. Recall also further necessary and sufficient conditions: the well-known Pepin's test, Wilson's Theorem, Lucas's Theorem for primality, etc., see [4].

In this paper, we establish a new necessary and sufficient condition for the primality of F_m. This condition is based on the observation that the set of primitive roots of a Fermat prime is equal to the set of all its quadratic non-residues. The necessity of this condition for the primality of F_m is well-known (see, e.g., [1, Problem 17(b), p. 222]), whereas its sufficiency is new to the authors' knowledge. For a paper dealing with similar topics as our paper but in the framework of graph theory, see [7].

2. Preliminaries

Recall that the Euler totient function φ at $n \in \mathbb{N} = \{1, 2, \ldots\}$ is defined as the number of all natural numbers not greater than n, which are coprime to n, i.e.,

$$\varphi(n) = |\{a \in \mathbb{N};\ 1 \leqslant a \leqslant n,\ \gcd(a, n) = 1\}|,$$

where $|\cdot|$ denotes the number of elements. It is easily seen that $\varphi(1) = 1$, $\varphi(2) = 1$, and that all other values of $\varphi(n)$ for $n > 2$ are even. If p is prime, then clearly

$$\varphi(p^s) = (p - 1)p^{s-1} \tag{2.1}$$

for every $s \in \mathbb{N}$. Moreover, φ is a multiplicative function in the sense that if $\gcd(a, b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$. Consequently, if the prime power factorization of N is given by

$$N = \prod_{i=1}^{r} p_i^{s_i},$$

where $p_1 < p_2 < \ldots < p_r$, $s_i > 0$, then

$$\varphi(N) = \prod_{i=1}^{r} (p_i - 1)p_i^{s_i - 1}. \tag{2.2}$$

It is easily observed from (2.1) and (2.2) that $\varphi(N) < N-1$ if and only if N is composite. Thus, we have the following lemma.

Lemma 2.1. *The Fermat number F_m is prime if and only if*

$$\varphi(F_m) = 2^{2^m}. \tag{2.3}$$

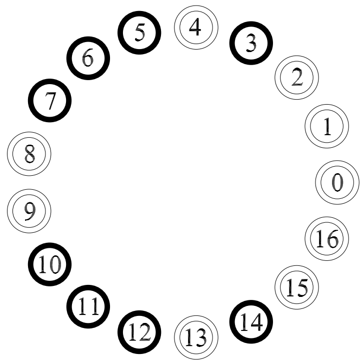
By the famous Euler's Theorem, the maximum possible order modulo n of any integer a coprime to n is equal to $\varphi(n)$, i.e.,

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

If a is an integer such that $\gcd(a, n) = 1$, then a is defined to be a *primitive root modulo n* if

$$a^j \not\equiv 1 \pmod{n} \quad \text{for all } j \in \{1, 2, \ldots, \varphi(n) - 1\}.$$

In Figure 1, we see the distribution of primitive roots modulo the Fermat prime F_2.



1. Primitive roots modulo 17 are indicated by the black color.

The next theorem determines all integers $m \geqslant 2$ which have primitive roots.

Theorem 2.2. *Let $m \geqslant 2$. There exists a primitive root modulo m if and only if $m \in \{2, 4, p^s, 2p^s\}$, where p is an odd prime and $s \geqslant 1$. Moreover, if m has a primitive root, then m has exactly $\varphi(\varphi(m))$ incongruent primitive roots.*

For the proof, see [1, pp. 160–164] or [6, pp. 102–104].

Definition 2.3. Let $n \geqslant 2$ and a be integers such that $\gcd(a, n) = 1$. If the quadratic congruence

$$x^2 \equiv a \pmod{n}$$

has a solution x, then a is called a *quadratic residue modulo n*. Otherwise, a is called a *quadratic non-residue modulo n*.

Proposition 2.4. *Every integer $n \geqslant 3$ has at least $\varphi(n)/2$ quadratic non-residues. If $n = p \geqslant 3$ is prime, it has precisely $\varphi(p)/2 = (p-1)/2$ quadratic non-residues.*

Proof. Set $A = \{a;\ 1 \leqslant a \leqslant n-1,\ \gcd(a,n) = 1\}$. Thus $|A| = \varphi(n)$. If $a \in A$, then also $-a \in A$ and $a^2 \in A$ after reduction modulo n. Modulo n, $a \not\equiv -a$ for each $a \in A$, because $2a \equiv 0$ for an $a \in A$ would imply that n divides 2. Also, $a \not\equiv b$ implies $-a \not\equiv -b$. When a runs through A, the squares a^2 reduced modulo n produce at most $\varphi(n)/2$ quadratic residues because $a^2 \equiv (-a)^2$. Hence, we have at least $\varphi(n)/2$ quadratic non-residues.

In the case $n = p$, both the bounds for quadratic residues and non-residues turn into equalities because, modulo p, $a^2 \equiv b^2$ is equivalent to $(a-b)(a+b) \equiv 0$, and since the modulus is prime, we have $a \equiv \pm b$. $\square$

3. Main results

For a natural number n set

$$M(n) = \{a \in \{1, \dots, n-1\};\ a \text{ is a primitive root modulo } n\}$$

and

$$\begin{aligned} K(n) = \{a \in \{1, \dots, n-1\};\ &\gcd(a,n) = 1 \\ &\text{and } a \text{ is a quadratic non-residue} \pmod n\}. \end{aligned}$$

Notice that $M(1) = K(1) = \emptyset$, $M(2) = \{1\}$, and $K(2) = \emptyset$.

Lemma 3.1. *If $n \geqslant 3$, then*

$$M(n) \subset K(n). \tag{3.1}$$

Proof. Let $n \geqslant 3$. Then $\varphi(n)$ is even. If $\gcd(n,a) = 1$ and $a \in \{1, \dots, n-1\}$ is a quadratic residue modulo n, then there exists an integer x such that

$$x^2 \equiv a \pmod n.$$

By Euler's Theorem,

$$a^{\varphi(n)/2} \equiv x^{\varphi(n)} \equiv 1 \pmod n,$$

and a is not a primitive root modulo n. Thus (3.1) holds. $\square$

Further we introduce a necessary and sufficient condition for the primality of Fermat numbers, which states that the sets $M(n)$ and $K(n)$ for an odd $n \geqslant 3$ are equal if and only if n is a Fermat prime (compare Figure 1). Later in Theorem 3.3, we show that $M(n) = K(n)$ for an even natural number n if and only if n equals 4 or two times a Fermat prime.

Theorem 3.2. *Let $n \geqslant 3$ be a positive odd integer. Then n is a Fermat prime if and only if $M(n) = K(n)$.*

P r o o f. Let $n = F_m$ be a Fermat prime. Then, by Theorem 2.2, (2.3), (2.1), and Proposition 2.4, we obtain

$$|M(F_m)| = \varphi(\varphi(F_m)) = \varphi(2^{2^m}) = 2^{2^m-1} = \frac{F_m - 1}{2} = |K(F_m)|. \tag{3.2}$$

Since $M(n)$ and $K(n)$ have the same cardinality by (3.2), we see by (3.1) that $M(n) = K(n)$.

Conversely, assume by way of contradiction that $n \geqslant 3$ is not a Fermat prime and that $M(n) = K(n)$. By Proposition 2.4,

$$|K(n)| \geqslant \frac{\varphi(n)}{2} \geqslant 1$$

for $n \geqslant 3$. Hence, $M(n) \neq \emptyset$, since $M(n) = K(n)$. It follows from Theorem 2.2 that $n = p^s$ for some odd prime p and a positive integer s.

Assume first that $s = 1$. Then there exist $k \geqslant 1$ and odd $q \geqslant 3$ such that

$$p - 1 = 2^k q, \tag{3.3}$$

(since if $q = 1$ and if $k = r\ell$ for $r \geqslant 3$ odd and $\ell \geqslant 1$, then $p = 2^{r\ell} q + 1$ is divisible by $2^\ell + 1$ and hence, composite). Then by Theorem 2.2, (2.1), (3.3), (2.2), (3.3) again, and Proposition 2.4, we obtain

$$\begin{aligned} |M(p)| &= \varphi(\varphi(p)) = \varphi(p-1) = \varphi(2^k q) = \varphi(2^k)\varphi(q) \\ &\leqslant 2^{k-1}(q-1) = \frac{1}{2}2^k(q-1) < \frac{p-1}{2} = |K(p)|. \end{aligned} \tag{3.4}$$

Hence, $M(p) \neq K(p)$.

Now assume that $s \geqslant 2$ and let $p - 1 = 2^k q$, where $k \geqslant 1$ and $q \geqslant 1$ is odd. By Proposition 2.4,

$$|K(p^s)| \geqslant \frac{\varphi(p^s)}{2} = \frac{(p-1)p^{s-1}}{2}. \tag{3.5}$$

Consequently, we obtain

$$
\begin{aligned}
(3.6)\qquad |M(p^s)| &= \varphi(\varphi(p^s)) = \varphi((p-1)p^{s-1}) = \varphi(2^k q)\varphi(p^{s-1}) \\
&= \varphi(2^k)\varphi(q)\varphi(p^{s-1}) = 2^{k-1}\varphi(q)(p-1)p^{s-2} \\
&< 2^{k-1}qp^{s-1} = \frac{(p-1)p^{s-1}}{2} \leqslant |K(p^s)|.
\end{aligned}
$$

From this and (3.4) we get

$$(3.7)\qquad |M(p^s)| < |K(p^s)| \quad \text{for } s \geqslant 1$$

and the theorem is therefore proved. □

Theorem 3.3. *Let n be a positive even integer. The number n is equal to 4 or to twice a Fermat prime if and only if $M(n) = K(n)$.*

Before proving Theorem 3.3, we will need the following lemma.

Lemma 3.4. *Suppose that $r \geqslant 3$ is odd. Then*

$$|M(2r)| = |M(r)| \quad \textit{and} \quad |K(2r)| = |K(r)|.$$

P r o o f. The first equality holds if $M(r)$ is empty by Theorem 2.2. So let $M(r) \neq \emptyset$. By Theorem 2.2, $r = p^s$ for an odd prime p and an integer $s \geqslant 1$, and $M(2r) \neq \emptyset$. Then using Theorem 2.2 again,

$$(3.8)\qquad |M(2r)| = \varphi(\varphi(2r)) = \varphi(\varphi(2)\varphi(r)) = \varphi(\varphi(r)) = |M(r)|.$$

Moreover, by Proposition 2.4, $K(r) \neq \emptyset$. Note that if $a \in \{1, \ldots, r\}$ is a quadratic non-residue modulo r such that $\gcd(a, r) = 1$, then exactly one of a and $a + r$ is odd, and hence exactly one of these two numbers is a quadratic non-residue modulo $2r$. It now follows that

$$|K(2r)| = |K(r)|.$$

From this and (3.8) we see that the lemma holds. □

P r o o f o f T h e o r e m 3.3. Obviously,

$$M(4) = \{3\} = K(4).$$

Further, let F_m be prime. According to (3.2), $|M(F_m)| = |K(F_m)|$. Hence, by Lemma 3.4, $|M(2F_m)| = |K(2F_m)|$ and thus, by (3.1), $M(2F_m) = K(2F_m)$.

Suppose on the contrary that $n \neq 4$, $n \neq 2F_m$, where F_m is prime, and $M(n) = K(n)$. First notice that $n \neq 2$, since $M(2) = \{1\}$ and $K(2) = \emptyset$.

Further, assume that $M(n) \neq \emptyset$. Then, by Theorem 2.2, $n = 2p^s$, where p is an odd prime, $s \geqslant 1$, and it is not the case that $s = 1$ and p is a Fermat number. According to (3.7), $|M(p^s)| < |K(p^s)|$, and thus by Lemma 3.4,

$$|M(2p^s)| < |K(2p^s)|.$$

Finally, suppose that $M(n) = \emptyset$ and $n \geqslant 6$. By Proposition 2.4, we have $K(n) \neq \emptyset$, and hence, $M(n) \neq K(n)$. □

The next theorem determines those integers $n \geqslant 2$ for which the cardinality of the set $K(n) \setminus M(n)$ is equal to 1.

Theorem 3.5. *Let $n \geqslant 2$ be an integer. Then*

$$|M(n)| = |K(n)| - 1 \tag{3.9}$$

if and only if $n = 9$, or $n = 18$, or either n or $n/2$ is equal to an odd prime p for which $(p-1)/2$ is also an odd prime. Moreover, if (3.9) holds, then $n - 1 \in K(n)$ but $n - 1 \notin M(n)$.

Proof. By Theorems 3.2 and 3.3, we may assume that $n \neq 4, F_m$, or $2F_m$, where F_m is prime. Also, clearly $n \neq 2$. Suppose first that $n = p$, where p is an odd prime which is not a Fermat number. Analogously to (3.3), let $p - 1 = 2^k q$, where $q \geqslant 3$ is odd and $k \geqslant 1$. Then, by Proposition 2.4, $|K(p)| = (p-1)/2 = 2^{k-1}q$. Moreover, by Theorem 2.2,

$$\begin{aligned}|M(p)| &= \varphi(\varphi(p)) = \varphi(p-1) = \varphi(2^k q) = \varphi(2^k)\varphi(q) = 2^{k-1}\varphi(q)\\ &\leqslant 2^{k-1}(q-1) = 2^{k-1}q - 2^{k-1} = |K(p)| - 2^{k-1} \leqslant |K(p)| - 1.\end{aligned}$$

Thus, $|M(p)| = |K(p)| - 1$ if and only if $\varphi(q) = q - 1$ and $k = 1$. This occurs if and only if $(p-1)/2 = q$, where q is an odd prime. Since $K(p) \neq \emptyset$, it now follows by Lemma 3.4 that for $n = 2p$, where p is an odd prime, we have $|M(2p)| = |K(2p)| - 1$ if and only if $(p-1)/2$ is an odd prime.

We next assume that $n = p^s$, where p is an odd prime and $s \geqslant 2$. Let $p - 1 = 2^k q$, where $q \geqslant 1$ is odd and $k \geqslant 1$. Then, by (3.6),

$$|M(p^s)| = 2^{k-1}\varphi(q)p^{s-2}(p-1) \leqslant 2^{k-1}qp^{s-1} - 2^{k-1}qp^{s-2}.$$

Moreover, by (3.5),

$$|K(p^s)| \geqslant \frac{(p-1)p^{s-1}}{2} = 2^{k-1}qp^{s-1}.$$

Hence, $|M(p^s)|$ can equal $|K(p^s)| - 1$ only if $\varphi(q) = q$ and $2^{k-1}qp^{s-2} = 1$. This can occur if and only if $q = k = 1$ and $s = 2$. Therefore, $p - 1 = 2$, which implies that $n = 3^2 = 9$. By inspection, we find that $K(9) = \{2, 5, 8\}$, $M(9) = \{2, 5\}$, and thus $|M(9)| = |K(9)| - 1$. Since $M(9) \neq \emptyset$, it follows by Lemma 3.4 that when $n = 2p^s$, where p is an odd prime and $s \geqslant 2$, then $|M(2p^s)| = |K(2p^s)| - 1$ if and only if $p = 3$ and $s = 2$, i.e., $n = 18$.

According to Theorem 2.2, the only remaining cases to consider are those for which $M(n) = \emptyset$. We will show that then $|K(n)| \geqslant 2$, and hence $|M(n)| \neq |K(n)| - 1$. By Theorem 2.2, if $M(n) = \emptyset$, then either $n = 2^s$, where $s \geqslant 3$, or $n = p^s t$, where p is an odd prime, $s \geqslant 1$, $\gcd(p, t) = 1$, and $t \geqslant 3$. Assume first that $n = 2^s$, where $s \geqslant 3$. Then, by Proposition 2.4 and (2.1),

$$|K(n)| \geqslant \frac{\varphi(2^s)}{2} = \frac{2^{s-1}}{2} \geqslant 2.$$

If $n = p^s t$, where p is an odd prime, $s \geqslant 1$, $\gcd(p, t) = 1$, and $t \geqslant 3$, then by Proposition 2.4 and (2.2),

$$|K(n)| \geqslant \frac{\varphi(p^s t)}{2} = \frac{\varphi(p^s)\varphi(t)}{2} \geqslant \frac{2 \cdot 2}{2} = 2.$$

Finally, to prove the last assertion, suppose that (3.9) holds and $n = 9$, or $n = 18$, or either n or $n/2$ is equal to an odd prime p for which $(p-1)/2$ is also an odd prime. One can check that if p is an odd prime such that $(p-1)/2$ is also an odd prime, then $p \equiv 3 \pmod 4$. Since n is divisible by a prime p such that $p \equiv 3 \pmod 4$, we have $n - 1 \in K(n)$, i.e., -1 is a quadratic non-residue. Clearly, $n - 1 \notin M(n)$, because $n \geqslant 7$ (thus $\varphi(n) > 2$) and $(n-1)^2 \equiv 1 \pmod n$. □

Remark 3.6. Odd primes p for which $2p + 1$ is also a prime are called *Sophie Germain primes*. By Theorem 3.5, $|M(n)| = |K(n)| - 1$ if and only if $n \in \{9, 18\}$ or either n or $n/2$ equals p, where $(p-1)/2$ is a Sophie Germain prime.

Remark 3.7. The set $M(F_m)$ for $m > 1$ consists of those numbers which are not powers of 2 modulo F_m.

A great amount of effort has been devoted to the investigation of the Fermat numbers for many years (see, e.g., [1–6] and references therein). Although we know hundreds of factors of the Fermat numbers and many necessary and sufficient conditions for the primality of F_m, we are not able to discover a general principle which would lead to a definitive answer to the question whether F_4 is the largest Fermat prime.

A c k n o w l e d g e m e n t. This paper was supported by the common Czech-US cooperative research project of the programme KONTACT No. ME 148 (1998). The authors thank very much the anonymous referee for his/her many helpful suggestions, which substantially simplified the paper.

References

[1] *Burton, D. M.*: Elementary Number Theory, fourth edition. McGraw-Hill, New York, 1998.
[2] *Crandall, R. E., Mayer, E., Papadopoulos, J.*: The twenty-fourth Fermat number is composite. Math. Comp. (submitted).
[3] *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.
[4] *Křížek, M., Luca, F., Somer, L.*: 17 Lectures on Fermat Numbers. From Number Theory to Geometry. Springer, New York, 2001.
[5] *Luca, F.*: On the equation $\varphi(|x^m - y^m|) = 2^n$. Math. Bohem. *125* (2000), 465–479.
[6] *Niven, I., Zuckerman, H. S., Montgomery, H. L.*: An Introduction to the Theory of Numbers, fifth edition. John Wiley and Sons, New York, 1991.
[7] *Szalay, L.*: A discrete iteration in number theory. BDTF Tud. Közl. VIII. Természettudományok 3., Szombathely (1992), 71–91. (In Hungarian.)
[8] *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.

Authors' addresses: *Michal Křížek*, Mathematical Institute, Academy of Sciences, Žitná 25, CZ-115 67 Praha 1, Czech Republic, e-mail: `krizek@math.cas.cz`; *Lawrence Somer*, Department of Mathematics, Catholic University of America, Washington, D.C. 20064, U.S.A., e-mail: `somer@cua.edu`.