Journal of Integer Sequences, Vol. 25 (2022),
Article 22.4.3

A Simple Proof of Skula's Theorem on Prime Power Divisors of Mersenne Numbers

Jiří Klaška
Institute of Mathematics
Faculty of Mechanical Engineering
Brno University of Technology
Technická 2
CZ – 616 69 Brno
Czech Republic
klaska@fme.vutbr.cz

Abstract

Recently, Skula proved an interesting result concerning the equivalence between higher order Wieferich primes and prime power divisors of Mersenne numbers. In the present paper, we provide a simple proof of Skula's result.

1 Introduction

The Mersenne numbers $M_n = 2^n - 1$, $n \in \mathbb{N}$ have been studied by many authors over past centuries, with a number of remarkable statements discovered and proved since the time of Marin Mersenne (1588–1648). See sequences A000225 and A001348 in the *On-Line Encyclopedia of Integer Sequences* [6].

The present paper is concerned with the connection between higher-order Wieferich primes and prime power divisors of Mersenne numbers. First, however, we recall certain definitions and facts relating to this topic. In 1997, Agoh, Dilcher, and Skula published the well-known paper [1] in which the concepts of Fermat quotient and Wieferich prime were extended substantially.

Let $a, m \in \mathbb{Z}$, $m \geq 2$ and let $\gcd(a, m) = 1$. By [1, Definition 1.2],

$$q(a, m) = \frac{a^{\varphi(m)} - 1}{m}$$

is called the Euler quotient of m with base a. From Euler's theorem it is clear (see for example [2, p. 33] or [4, p. 42]) that $q(a,m) \in \mathbb{Z}$. By [1, Definition 1.2], m is called a Wieferich number with base a if $q(a,m) \equiv 0 \pmod{m}$. See also [6, A077816]. Specifically, if p is a prime satisfying $q(2,p) \equiv 0 \pmod{p}$, we obtain the well-known definition of a Wieferich prime: p is a Wieferich prime if $2^{p-1} \equiv 1 \pmod{p^2}$. See [6, A001220]. By [5, Definition 1.4] a Wieferich prime p is called a Wieferich prime of order $n \in \mathbb{N}$ if

$$q(2,p^n) \equiv 0 \pmod{p^n} \quad \text{or, equivalently,} \quad 2^{p^{n-1}(p-1)} \equiv 1 \pmod{p^{2n}}.$$

Hence, a prime p is a Wieferich one if and only if p is Wieferich prime of order 1 and, p is a Wieferich prime of order n if and only if p^n is a Wieferich number with base 2.

Finally, let us recall that the smallest positive integer h for which $a^h \equiv 1 \pmod{m}$ is called the multiplicative order of a modulo m, which we write as $h = \mathrm{ord}_m(a)$. Now we can formulate the main result presented in [5].

Theorem 1 (Skula, 2019)**.** *Let $n \in \mathbb{N}$ and let p, q be odd primes. If $p^n | M_q$, then the following statements are equivalent:*

(A) $p^{n+1} | M_q$.

(B) *p is a Wieferich prime of order n.*

(C) $\mathrm{ord}_{p^{n+1}}(2) = q$.

The proof of Theorem 1 given in [5] is mainly based on some special properties of Euler quotient, such as the logarithm property presented in [5, Proposition 1.1] or the proposition on the Euler quotient for two bases [5, Proposition 2.1]. Furthermore, the proof in [5] uses the results [1, Lemma 5.1] and [1, Corollary 5.2] on the order of the number $q(2,p)$ modulo p within the meaning of definition [2, p. 3]. Hence, the proof of Theorem 1 in [5] is the result of resourcefully applying a series of findings.

The main purpose of this paper is to show that Theorem 1 can be proved in a way simpler than the one in [5], that is, without using special propositions on the Euler quotient.

2 Proof of Theorem 1

We begin by recalling some of the known properties of $\mathrm{ord}_m(a)$, which are needed in our proof of Theorem 1.

Lemma 2. *Let $a, m \in \mathbb{Z}$, $m \geq 2$ and let $\gcd(a,m) = 1$. Then* (i)–(vii) *holds.*

(i) *Let $k \in \mathbb{N}$. Then $a^k \equiv 1 \pmod{m}$ if and only if $\mathrm{ord}_m(a) | k$.*

(ii) $\mathrm{ord}_m(a) | \varphi(m)$. *Consequently, if p is an odd prime, then $\mathrm{ord}_p(2) | p-1$.*

(iii) *Let $a, k, n \in \mathbb{N}$ and let p be an odd prime satisfying $p \nmid a$. Further, let* $\operatorname{ord}_p(a) = h$ *and let* $p^k \| a^h - 1$. *Then*

$$\operatorname{ord}_{p^n}(a) = \begin{cases} h, & \text{for } n \leq k; \\ p^{n-k}h, & \text{for } n > k. \end{cases}$$

Here, $p^k \| a^h - 1$ *means that* $p^k | a^h - 1$ *but* $p^{k+1} \nmid a^h - 1$.

(iv) *Let $a, n \in \mathbb{N}$ and let p be an odd prime satisfying $p \nmid a$. If* $\operatorname{ord}_{p^n}(a) = h$, *then* $\operatorname{ord}_{p^{n+1}}(a) \in \{h, ph\}$. *Consequently,* $\operatorname{ord}_{p^n}(a) | \operatorname{ord}_{p^{n+1}}(a)$.

(v) *Let $k, n \in \mathbb{N}$ and let p be an odd prime. If* $\operatorname{ord}_p(2) = \cdots = \operatorname{ord}_{p^n}(2) \neq \operatorname{ord}_{p^{n+1}}(2)$, *then* $\operatorname{ord}_{p^{n+k}}(2) = p^k \operatorname{ord}_p(2)$.

(vi) *Let $n \in \mathbb{N}$ and let p be an odd prime. If* $\operatorname{ord}_{p^n}(2) | p - 1$, *then* $\operatorname{ord}_{p^k}(2) = \operatorname{ord}_{p^n}(2)$ *for any* $k \in \{1, \ldots, n\}$.

(vii) *Let $n \in \mathbb{N}$ and let p, q be odd primes. If* $\operatorname{ord}_{p^n}(2) | q$, *then* $\operatorname{ord}_{p^k}(2) = q$ *for any* $k \in \{1, \ldots, n\}$.

The proofs of (i) and (ii) can be found in [4, p. 43]. Part (iii) is Theorem 4.4 proved by LeVeque in [3, pp. 80–81]. See also Theorem 4–6 in [4, pp. 52–53]. Part (iv) immediately follows from (iii). Part (v) is a direct consequence of (iii) for $p = 2$. Finally, (vi) and (vii) follow from (iv).

Proposition 3. *Let $n \in \mathbb{N}$ and let p be a prime. Then,*

$$2^{p^{n-1}(p-1)} \equiv 1 \pmod{p^{2n}} \quad \text{if and only if} \quad 2^{p-1} \equiv 1 \pmod{p^{n+1}}. \tag{1}$$

Proof. Let us first assume that p is an odd prime.

Let $2^{p^{n-1}(p-1)} \equiv 1 \pmod{p^{2n}}$. Applying (i), we obtain

$$\operatorname{ord}_{p^{2n}}(2) | p^{n-1}(p-1). \tag{2}$$

Suppose that $2^{p-1} \not\equiv 1 \pmod{p^{n+1}}$. From (i), it now follows that $\operatorname{ord}_{p^{n+1}}(2) \nmid p - 1$ and, by (ii), $\operatorname{ord}_p(2) | p - 1$. This means that $\operatorname{ord}_{p^{n+1}}(2) \neq \operatorname{ord}_p(2)$. From (v), it follows that there exists an $s \in \{1, \ldots, n\}$ such that $\operatorname{ord}_{p^{n+1}}(2) = p^s \operatorname{ord}_p(2)$. Hence,

$$\operatorname{ord}_{p^{2n}}(2) = p^n \operatorname{ord}_{p^{n+1}}(2) = p^{n+s} \operatorname{ord}_p(2). \tag{3}$$

Combining (3) and (2), we obtain $p^{n+s} \operatorname{ord}_p(2) | p^{n-1}(p-1)$. Since $s \in \{1, \ldots, n\}$ and $\operatorname{ord}_p(2) | p - 1$, we have a contradiction.

Conversely, let $2^{p-1} \equiv 1 \pmod{p^{n+1}}$. Then, by (i), we have $\operatorname{ord}_{p^{n+1}}(2) | p - 1$ and, using (vi), we obtain $\operatorname{ord}_{p^{n+1}}(2) = \operatorname{ord}_p(2)$. Further, by (v), there exist a $t \in \{0, \ldots, n-1\}$ such that

$$\operatorname{ord}_{p^{2n}}(2) = p^t \operatorname{ord}_{p^{n+1}}(2) = p^t \operatorname{ord}_p(2). \tag{4}$$

Since $t \leq n-1$, (4) implies $\mathrm{ord}_{p^{2n}}(2) | p^{n-1} \mathrm{ord}_p(2)$, which, together with $\mathrm{ord}_p(2) | p-1$, yields $\mathrm{ord}_{p^{2n}}(2) | p^{n-1}(p-1)$. Hence, $2^{p^{n-1}(p-1)} \equiv 1 \pmod{p^{2n}}$.

Finally, let $p = 2$. Then, for any $n \in \mathbb{N}$, $2^{2^{n-1}} \not\equiv 1 \pmod{2^{2n}}$ and $2 \not\equiv 1 \pmod{2^{n+1}}$. This means that, (1) holds for $p = 2$ as well. The proof is now complete. □

Proposition 4. *Let $n \in \mathbb{N} \cup \{0\}$ and let p be an odd prime. Then,*

$$2^{p-1} \equiv 1 \pmod{p^{n+1}} \quad \textit{if and only if} \quad \mathrm{ord}_{p^{n+1}}(2) = \mathrm{ord}_p(2).$$

Proof. Let $2^{p-1} \equiv 1 \pmod{p^{n+1}}$. Then, by (i), $\mathrm{ord}_{p^{n+1}}(2) | p-1$. Next, applying (iii), we obtain $\mathrm{ord}_{p^{n+1}}(2) = p^s \mathrm{ord}_p(2)$ for some $s \in \{0, \ldots, n\}$. Suppose that $s \neq 0$. Then, $p^s \mathrm{ord}_p(2) | p-1$, which is a contradiction. Hence, $\mathrm{ord}_{p^{n+1}}(2) = \mathrm{ord}_p(2)$.

Conversely, let $\mathrm{ord}_{p^{n+1}}(2) = \mathrm{ord}_p(2) = h$. Then, by (ii), $h | p-1$. This means that there exists a $k \in \mathbb{N}$ such that $p-1 = hk$. Since $2^h \equiv 1 \pmod{p^{n+1}}$, we have $2^{p-1} = 2^{hk} = (2^h)^k \equiv 1 \pmod{p^{n+1}}$, as required. □

Now we are ready to prove Theorem 1.

Proof. First, we show that (A) implies (B). Let $p^{n+1} | M_q$. Then, $2^q \equiv 1 \pmod{p^{n+1}}$ which yields $\mathrm{ord}_{p^{n+1}}(2) | q$. Applying (vii), we obtain $\mathrm{ord}_{p^{n+1}}(2) = \mathrm{ord}_p(2) = q$. This means, by Proposition 4, that $2^{p-1} \equiv 1 \pmod{p^{n+1}}$ and, using Proposition 3, we conclude that p is a Wieferich prime of order n.

Next, we show that (B) implies (C). Assume that p is a Wieferich prime of order n. Then, by Proposition 3, $2^{p-1} \equiv 1 \pmod{p^{n+1}}$ and, using (i), we get $\mathrm{ord}_{p^{n+1}}(2) | p-1$. Next, from the basic assumption $p^n | M_q$, we obtain $2^q \equiv 1 \pmod{p^n}$ and, by (i), we get $\mathrm{ord}_{p^n}(2) | q$. Since q is an odd prime and $\mathrm{ord}_{p^n}(2) \neq 1$, we have $\mathrm{ord}_{p^n}(2) = q$. Hence, by (iv), $\mathrm{ord}_{p^{n+1}}(2) = pq$ or $\mathrm{ord}_{p^{n+1}}(2) = q$. Suppose that $\mathrm{ord}_{p^{n+1}}(2) = pq$. Since $\mathrm{ord}_{p^{n+1}}(2) | p-1$, we get $pq | p-1$, a contradiction.

Finally, we show that (C) implies (A). Let $\mathrm{ord}_{p^{n+1}}(2) = q$. Then, $2^q \equiv 1 \pmod{p^{n+1}}$, which yields $p^{n+1} | M_q$. The proof is complete. □

3 Acknowledgments

The author thanks the anonymous referee for carefully reading the manuscript.

References

[1] T. Agoh, K. Dilcher, and L. Skula, Fermat quotients for composite moduli, *J. Number Theory* **66** (1997), 29–50.

[2] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, 2nd edition, Springer-Verlag, 1992.

[3] W. J. LeVeque, *Fundamentals of Number Theory*, Addison-Wesley, 1977.

[4] W. J. LeVeque, *Topics in Number Theory*, Volume I, Dover Publications, 2002.

[5] L. Skula, Prime power divisors of Mersenne numbers and Wieferich primes of higher order, *Integers* **19** (2019), #A19.

[6] N. J. A. Sloane et al., *The On-Line Encyclopedia of Integer Sequences*, available at https://oeis.org, 2022.

2020 *Mathematics Subject Classification*: Primary 11A41; Secondary 11A07.
Keywords: Mersenne number, Wieferich number, Wieferich prime.

(Concerned with sequences A000225, A001220, A001348, and A077816.)

Received January 27 2022; revised version received March 29 2022. Published in *Journal of Integer Sequences*, March 31 2022.

Return to Journal of Integer Sequences home page.