PRIME POWER DIVISORS OF MERSENNE NUMBERS AND WIEFERICH PRIMES OF HIGHER ORDER

Ladislav Skula[1]
Institute of Mathematics,Faculty of Mechanical Engineering, Brno University of Technology, Brno, Czech Republic
skula@fme.vutbr.cz

Received: 12/6/17, Revised: 8/16/18, Accepted: 2/2/19, Published: 3/15/19

Abstract

The equivalence is presented between a *Wieferich* prime p of order n and the divisibility of the *Mersenne* number M_q by the power p^{n+1}.

1. Introduction

Throughout this paper, a, n, and m will denote positive integers, with $m \geq 2$, and p an odd prime. If the integer a is not divisible by p, then Fermat's Little Theorem states that

$$a^{p-1} \equiv 1 \pmod{p}.$$

This theorem guarantees that the number

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

is an integer which is called the *Fermat quotient of* p *with base* a. This notion can be extended for a composite integer m and an integer a where m and a are relatively prime integers. By Euler's Theorem we have

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

The integer

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

is called the *Euler quotient of* m *with base* a, where φ means Euler's totient function.

A whole range of results on Fermat and Euler quotions is known, the following Proposition on the "logarithm property" being of special importance.

[1] *Mathematics Subject Classification.* Primary: 11A41; Secondary: 11A07
Keywords and phrases. Wieferich prime of order n, *Mersenne* number, *Fermat* and *Euler* quotient

Proposition 1.1. *Let b be an integer, $(a,m)=(b,m)=1$. Then,*

$$q(a\cdot b,m)\equiv q(a,m)+q(b,m) \pmod{m}.$$

Remark 1.2. For $m=p$ (p prime), this property was proved by Eisenstein [4], for m odd ($m\geq 1$) by Lerch [5], and generally by Agoh, Dilcher, Skula [1], Proposition 2.1 (a).

Wieferich [7], in his criterion on the first case of Fermat Last Theorem for exponent p, used the following property of p: $q(2,p)\equiv 0 \pmod{p}$, or equivalently $2^{p-1}\equiv 1 \pmod{p^2}$. For this reason, p with this property is called a *Wieferich prime*. At present, only two Wieferich primes, 1093 and 3511, are known and no prime $p<6.7\times 10^{15}$ except these primes is Wieferich [3].

In [1], Definition 1.3, the notion of Wieferich prime was generalized as follows.

Definition 1.3. Let m and a be relatively prime integers. We say that m is a *Wieferich number with base a* if $q(a,m)\equiv 0 \pmod{m}$.

In the present paper we will only be concerned with the case $m=p^n$ and $a=2$.

Definition 1.4. Let the prime p be a Wieferich prime. Then p is called a *Wieferich prime of order n* if $q(2,p^n)\equiv 0 \pmod{p^n}$, or equivalently $2^{p^{n-1}(p-1)}\equiv 1 \pmod{p^{2n}}$.

From [1], Corollary 5.2, $(\mathrm{ord}_p(q(2,p^n)) = \mathrm{ord}_p(q(2,p)))$ we get any Wieferich prime is a Wieferich prime of order 1. (S.Proposition 2.2.)

The goal of the paper is to present the connection of a Wieferich prime p of order n with the divisibility of the Mersenne number $M_q=2^q-1$ by the prime power p^n, where q means a prime.

A. Rotkiewicz [6], and CH. K. Caldwell [2] proved that, if p is a prime and p^2 divides a Mersenne number M_q for a prime q, then p is a Wieferich prime. In the present paper we generalize this result and prove the other direction of this assertion as well.

2. Auxiliary Assertions

Proposition 2.1 (Statement on the Euler quotient for two bases). *Let m,N be relatively prime positive integers, and let r,Q be integers $1\leq r<m,\ Q>0$ with the property $N=m\cdot Q+r$. Then,*

$$N\cdot q(N,m)\equiv \varphi(m)\cdot Q+r\cdot q(r,m) \pmod{m}.$$

Proof. Suppose that m,N,r,Q are integers fulfilling the conditions in the Proposition. We have

$$N^{\varphi(m)}=\sum_{k=0}^{\varphi(m)}\binom{\varphi(m)}{k}(mQ)^k r^{\varphi(m)-k}\equiv r^{\varphi(m)}+\varphi(m)mQ^{\varphi(m)-1} \pmod{m^2}.$$

Since $q(N,m) = \frac{N^{\varphi(m)}-1}{m}$ and $N \equiv r \pmod{m}$, we get

$$mq(N,m) \equiv r^{\varphi(m)} - 1 + \varphi(m)mQN^{\varphi(m)-1} \pmod{m^2},$$

therefore

$$q(N,m) \equiv q(r,m) + \varphi(m)QN^{\varphi(m)-1} \pmod{m},$$

and hence

$$Nq(N,m) \equiv \varphi(m)Q + rq(r,m) \pmod{m}.$$

□

By [1], Corollary 5.2, we get:

Proposition 2.2. *We have* $\mathrm{ord}_p(q(2,p)) \geq n$*, or equivalently* $2^{p-1} \equiv 1 \pmod{p^{n+1}}$*, if and only if* p *is a Wieferich prime of order* n*.*

Lemma 2.3. *Let* q *be a prime,* $p^n | M_q$*, and let* δ *be the order of* $2 \pmod{p^{n+1}}$*. Then* $\delta = q$ *if and only if* $p^{n+1} | M_q$*; and* $\delta = q \cdot p$ *otherwise.*

Proof. We have $2^\delta \equiv 1 \pmod{p^{n+1}}$ and $2^q \equiv 1 \pmod{p^n}$. Therefore, the order of $2 \pmod{p^n}$ is q and $2^\delta \equiv 1 \pmod{p^n}$, hence $q|\delta$. There exists a positive integer T such that $2^q = 1 + p^N T$, thus

$$2^{qp} = \sum_{k=0}^{p} \binom{p}{k} p^{nk} \cdot T^k \equiv 1 \pmod{p^{n+1}},$$

and then $\delta \in \{q, p, q \cdot p\}$. If $\delta = p$, then $1 \equiv 2^\delta = 2 \cdot 2^{p-1} \equiv 2 \pmod{p}$, which is a contradiction. □

3. Main Theorem

Main Theorem 3.1. *Let* q *be a prime and let* p^n *divide* M_q*, where* $M_q = 2^q - 1$ *is a Mersenne number. Then, the following statements are equivalent:*

(a) p^{n+1} *divides* M_q*,*

(b) p *is a Wieferich prime of order* n*,*

(c) the order of $2 \pmod{p^{n+1}}$ *is* q*.*

Proof. We show the implication (a) $\Rightarrow$ (b). Let p^{n+1} divide M_q and let the order of $2 \pmod{p^{n+1}}$ be δ. Then, by Lemma 2.3, $\delta = q$, hence $2^q \equiv 1 \pmod{p^n}$. Using Euler's Theorem, we get

$$2^{\varphi(p^{n+1})} \equiv 1 \pmod{p^{n+1}}, \text{ therefore } 2^{p^n(p-1)} \equiv 1 \pmod{p^{n+1}}$$

and $q|p^n(p-1)$, therefore $q|(p-1)$. Then, there exists a positive integer x such that $p-1 = q \cdot x$. Hence $2^{p-1} = 2^{q \cdot x} \equiv 1 \pmod{p^{n+1}}$ and $\mathrm{ord}_p(2^{p-1}-1) \geq n+1$, and therefore

$$\mathrm{ord}_p \frac{2^{p-1}-1}{p} \geq n.$$

By Proposition 2.2, we get that p is a Wieferich prime of order n.

We prove the implication (b) $\Rightarrow$ (a). Assume that p is a Wieferich prime of order n. Set $m = p^n$ and $N = 2^q$. Since $2^q \equiv 1 \pmod{p^n}$, there exists a positive integer Q such that $N = m \cdot Q + 1$. Using Proposition 2.1 (Euler quotient for two bases) and Proposition 1.1 (logarithm property), we obtain

$$q \cdot 2^q \cdot q(2, p^n) \equiv -p^{n-1} \cdot Q \pmod{p^n}.$$

From the assumption that p is a Wieferich prime of order n, we get the congruence $0 \equiv q(2, p^n) \pmod{p^n}$, therefore $p|Q$ and then

$$2^q = p^{n+1} \cdot \frac{Q}{p} + 1 \equiv 0 \pmod{p^{n+1}},$$

hence $p^{n+1}|M_q$.

Lemma 2.3 gives the equivalence of statements (a) and (c). □

References

[1] T. Agoh, K. Dilcher and L. Skula, Fermat Quotients for Composite Moduli, *J. Number Theory*, **66** (1997), 29-50.

[2] CH. K. Caldwell, Proof that all prime-squared Mersenne divisors are Wieferich. https://primes.utm.edu/notes/proofs/SquareMerDiv.html.

[3] F. G. Dorais and D. Klyve, A Wieferich prime search up to $p < 6.7 \times 10^{15}$, *J. Integer Seq.* **14** (2011), 1-14.

[4] G. Eisenstein, Eine neue Gattung, zahlentheoretischer Funktionen, welche von zwei Elementen abhängen und durch gewisse lineare Funktional-Gleichungen definiert werden, *Math. Werke*, Gotthold Eisenstein, Band II, Chelsea, New York, 2nd ed. 1989, pp.705-711(710).

[5] M. Lerch, Zur Theorie des Fermatschen Quotienten $(a^{p-1}-1)/p = q(a)$, *Math. Ann.* **60** (1905), 471-490.

[6] A. Rotkiewicz, Sur les nombres de Mersenne dpourvus de facteurs carrs et sur les nombres naturels n tels que $n^2|2^n-2$, *Matem. Vesnik (Beograd)*, **2**(17), (1965), 78-80.

[7] A. Wieferich, Zum letzten Fermat'schen Theorem, *J. Reine Angew. Math.* **136** (1909), 293-302.