Indian J. Pure Appl. Math., **49**(3): 521-526, September 2018
 DOI: 10.1007/s13226-018-0281-8

A CONGRUENCE RELATION OF THE CATALAN-MERSENNE NUMBERS[1]

Ick Sun Eum

Department of Mathematics Education, Dongguk University-Gyeongju
123 *Dongdae-ro, Gyeongju, Gyeongbuk*, 38066, *South Korea*
e-mail: zandc@dongguk.ac.kr

(*Received* 16 *August* 2017; *accepted* 6 *October* 2017)

The Catalan-Mersenne numbers c_n are double Mersenne numbers defined by $c_0 = 2$ and $c_n = 2^{c_{n-1}} - 1$ for positive integers n. We prove a certain congruence relation of the Catalan-Mersenne numbers.

Key words : Mersenne number; congruences.

1. INTRODUCTION

Let $c_0 = 2$. For a positive integer n, the *n-th Catalan-Mersenne number* is defined by

$$c_n = 2^{c_{n-1}} - 1.$$

In 1876 Lucas proved that $c_4 = 2^{127} - 1$ is also a prime by using his primality test, known as the Lucas-Lehmer test [2, 3]. In 1876 and 1891 Catalan [1] noticed that the Mersenne numbers

$$\begin{aligned} c_1 &= 2^2 - 1 = 3, \\ c_2 &= 2^3 - 1 = 7, \\ c_3 &= 2^7 - 1 = 127, \\ c_4 &= 2^{127} - 1 = 170141183460469231731687303715884105727 \end{aligned}$$

were all primes and he conjectured that the numbers c_1, c_2, c_3, c_4, c_5, ... are all primes "up to a certain limit". But it is not known whether or not the 5th Catalan-Mersenne number c_5 is prime because it is too huge.

[1]This work was supported by the Dongguk University Research Fund of 2017 and the National Research Foundation of Korea(NRF) grant funded by the Korea government(MSIT) (No. NRF-2017R1C1B5017567).

Fermat's little theorem implies that if m is prime, then the Mersenne number $M_m = 2^m - 1$ satisfies

$$M_m \equiv 1 \pmod{m}. \tag{1}$$

The converse does not hold in general. In this paper, we shall prove that the congruence (1) also holds for all double Mersenne numbers. Moreover we shall show that the Catalan-Mersenne numbers satisfy stronger congruence relation than (1).

2. Congruence Relations

The numbers of the form $M_{M_n} = 2^{M_n} - 1$ are called double Mersenne numbers. From the definition, the Catalan-Mersenne numbers are a special case of the double Mersenne numbers. First, we introduce the following proposition.

Proposition 2.1 — Let p be a positive integer.

(i) M_p is a prime only if the exponent p is a prime.

(ii) Suppose that p is an odd prime. Then every prime divisor of M_p is of the form $2pk + 1$. Moreover, M_p is also of the same form, that is, $M_p = 2ph + 1$ for some positive integer h.

Proof : See [4, Chapter 7, §7.3]. □

Remark 2.2 : (i) When the exponent p is not a prime, Proposition 2.1 (ii) does not hold in general. For instance, we have $2^6 - 1 = 63 = 2 \cdot 31 + 1$ which is not of the form $2 \cdot 6h + 1$.

(ii) However, we will see in the following proposition that a part of Proposition 2.1 (ii) still valid for all double Mersenne numbers.

Proposition 2.3 — Let p be an odd prime. Let $M_{p,1} = M_p$ and $M_{p,n+1} = 2^{M_{p,n}} - 1$ for positive integers n. Then we have

$$M_{p,n+1} \equiv 1 \pmod{M_{p,n}}. \tag{2}$$

Proof : To show this, we will use induction on n. Since p is an odd prime, by Proposition 2.1 (ii), $M_{p,1} = M_p = 2ph + 1$ for some positive integer h. We note that

$$\begin{aligned} M_{p,2} - 1 &= 2^{M_{p,1}} - 2 = 2^{2ph+1} - 2 = 2((2^p)^{2h} - 1) \\ &= 2(2^p - 1)\left((2^p)^{2h-1} + (2^p)^{2h-2} + \cdots + (2^p)^1 + 1\right) \\ &= 2M_{p,1}\left((2^p)^{2h-1} + (2^p)^{2h-2} + \cdots + (2^p)^1 + 1\right) \\ &\equiv 0 \pmod{M_{p,1}}. \end{aligned}$$

Now, we suppose that the congruence (2) holds for n. Then there is a positive integer k such that $M_{p,n+1} = 2M_{p,n}k + 1$. From the induction hypothesis, we have

$$\begin{aligned} M_{p,n+2} - 1 &= 2^{M_{p,n+1}} - 2 = 2^{2M_{p,n}k+1} - 2 = 2\left((2^{M_{p,n}})^{2k} - 1\right) \\ &= 2(2^{M_{p,n}} - 1)\left((2^{M_{p,n}})^{2k-1} + (2^{M_{p,n}})^{2k-2} + \cdots + (2^{M_{p,n}})^1 + 1\right) \\ &= 2M_{p,n+1}\left((2^{M_{p,n}})^{2k-1} + (2^{M_{p,n}})^{2k-2} + \cdots + (2^{M_{p,n}})^1 + 1\right) \\ &\equiv 0 \pmod{M_{p,n+1}}. \end{aligned}$$

Hence, the congruence (2) also holds for $n+1$ and this proves our proposition. □

Example 2.4 : Let $p = 11$. Then the Mersenne number $2^{11} - 1 = 23 \cdot 89$ is composite. But, by Proposition 2.3, we get

$$2^{2^{11}-1} - 1 \equiv 1 \pmod{2^{11} - 1}.$$

Moreover, the Catalan-Mersenne numbers satisfy the following stronger congruence than (2).

***Theorem* 2.5** — *Let $m_0 = 1$. For each positive integer n there exists a positive integer m_n such that*

$$m_{n-1} | m_n \quad \textit{and} \quad c_{n+1} = 2m_n \prod_{i=1}^{n} c_i^{n+1-i} + 1 = 2c_1^n \cdot c_2^{n-1} \cdots c_{n-1}^2 \cdot c_n \cdot m_n + 1. \tag{3}$$

In other words,

$$c_{n+1} \equiv 1 \pmod{2c_1^n \cdot c_2^{n-1} \cdots c_{n-1}^2 \cdot c_n}. \tag{4}$$

PROOF : We will prove (3) by using induction on n. First, one can see that

$$\begin{aligned} c_2 &= 2^{c_1} - 1 = 2^3 - 1 = 7 = 2 \cdot 3 \cdot 1 + 1 = 2 \cdot c_1 \cdot 1 + 1, \\ c_3 &= 2^{c_2} - 1 = 2^7 - 1 = 127 = 2 \cdot 3^2 \cdot 7 \cdot 1 + 1 = 2 \cdot c_1^2 \cdot c_2 \cdot 1 + 1. \end{aligned}$$

This shows that $m_1 = 1$, $m_2 = 1$, $m_0 | m_1$ and $m_1 | m_2$. Thus (3) holds for $n = 1, 2$.

Now we suppose that (3) holds for n and $n+1$. Then, by induction hypothesis, there are positive integers m_n and m_{n+1} such that

$$m_n | m_{n+1}, \quad c_{n+1} = 2m_n \prod_{i=1}^{n} c_i^{n+1-i} + 1 \quad \text{and} \quad c_{n+2} = 2m_{n+1} \prod_{i=1}^{n+1} c_i^{n+2-i} + 1. \tag{5}$$

Since $m_n | m_{n+1}$, we have $(c_{n+1}-1) \mid (c_{n+2}-1)$ and

$$\frac{c_{n+2}-1}{c_{n+1}-1} = c_1 \cdot c_2 \cdots c_{n+1} \cdot \frac{m_{n+1}}{m_n} \in \mathbb{Z}.$$

From the definition, we derive that

$$\begin{aligned} c_{n+3}-1 &= 2(2^{c_{n+2}-1}-1) \\ &= 2(2^{(c_{n+1}-1)\frac{c_{n+2}-1}{c_{n+1}-1}}-1) \\ &= 2(2^{c_{n+1}-1}-1) \cdot \sum_{k=0}^{\frac{c_{n+2}-1}{c_{n+1}-1}-1} \left(2^{c_{n+1}-1}\right)^k \\ &= (c_{n+2}-1) \cdot \sum_{k=0}^{\frac{c_{n+2}-1}{c_{n+1}-1}-1} \left(2^{c_{n+1}-1}\right)^k . \end{aligned}$$

Therefore, we have $(c_{n+2}-1) | (c_{n+3}-1)$. Since $c_{n+2}-1 = 2m_{n+1}\prod_{i=1}^{n+1} c_i^{n+2-i}$, it remains to show that

$$\sum_{k=0}^{\frac{c_{n+2}-1}{c_{n+1}-1}-1} \left(2^{c_{n+1}-1}\right)^k \equiv 0 \pmod{c_1 \cdot c_2 \cdots c_{n+1} \cdot c_{n+2}}.$$

By (5), we have

$$2^{c_{n+1}-1} = \frac{c_{n+2}+1}{2} = m_{n+1}\prod_{i=1}^{n+1} c_i^{n+2-i} + 1 \equiv 1 \pmod{\prod_{i=1}^{n+1} c_i},$$

which implies that

$$\sum_{k=0}^{\frac{c_{n+2}-1}{c_{n+1}-1}-1} \left(2^{c_{n+1}-1}\right)^k \equiv \sum_{k=0}^{\frac{c_{n+2}-1}{c_{n+1}-1}-1} 1 \equiv \frac{c_{n+2}-1}{c_{n+1}-1} \equiv c_1 \cdot c_2 \cdots c_{n+1} \cdot \frac{m_{n+1}}{m_n} \equiv 0 \pmod{\prod_{i=1}^{n+1} c_i}.$$

On the other hand,

$$\begin{aligned} c_{n+3}-1 &= 2(2^{c_{n+2}-1}-1) \\ &= 2((2^{c_{n+1}})^{\frac{c_{n+2}-1}{c_{n+1}}}-1) \qquad \text{since } c_{n+1} | c_{n+2}-1 \text{ by (5)} \\ &= 2(2^{c_{n+1}}-1) \cdot \sum_{k=0}^{\frac{c_{n+2}-1}{c_{n+1}}-1} (2^{c_{n+1}})^k \\ &= 2c_{n+2} \cdot \sum_{k=0}^{\frac{c_{n+2}-1}{c_{n+1}}-1} (2^{c_{n+1}})^k \\ &\equiv 0 \pmod{c_{n+2}}. \end{aligned}$$

Since $\gcd(c_{n+2}, c_{n+2}-1) = 1$, c_{n+2} divides

$$\frac{c_{n+3}-1}{c_{n+2}-1} = \sum_{k=0}^{\frac{c_{n+2}-1}{c_{n+1}-1}-1} \left(2^{c_{n+1}-1}\right)^k.$$

Also, since $\gcd(c_{n+2}, c_i) = 1$ for $1 \le i \le n+1$ by (5), we can conclude that

$$c_1 \cdot c_2 \cdots c_{n+1} \cdot c_{n+2} \quad \text{divides} \quad \sum_{k=0}^{\frac{c_{n+2}-1}{c_{n+1}-1}-1} \left(2^{c_{n+1}-1}\right)^k.$$

Therefore, there exists a positive integer $\widetilde{m}_{n+2}$ so that

$$\sum_{k=0}^{\frac{c_{n+2}-1}{c_{n+1}-1}-1} \left(2^{c_{n+1}-1}\right)^k = c_1 \cdot c_2 \cdots c_{n+1} \cdot c_{n+2} \cdot \widetilde{m}_{n+2}.$$

Put $m_{n+2} = m_{n+1}\widetilde{m}_{n+2}$. Combining the above results, we obtain that

$$\begin{aligned} c_{n+3}-1 &= (c_{n+2}-1) \cdot \sum_{k=0}^{\frac{c_{n+2}-1}{c_{n+1}-1}-1} \left(2^{c_{n+1}-1}\right)^k \\ &= \left(2m_{n+1}\prod_{i=1}^{n+1} c_i^{n+2-i}\right) \cdot (c_1 \cdot c_2 \cdots c_{n+1} \cdot c_{n+2} \cdot \widetilde{m}_{n+2}) \\ &= 2m_{n+1}\widetilde{m}_{n+2}\prod_{i=1}^{n+2} c_i^{n+3-i} \\ &= 2m_{n+2}\prod_{i=1}^{n+2} c_i^{n+3-i}. \end{aligned}$$

By construction, $m_{n+1} | m_{n+2}$ and (3) also holds for $n+2$. This proves our assertion. □

Example 2.6 : For the case when $n = 1$, 2 and 3, we have

$$\begin{aligned} c_2 &= 2^{c_1} - 1 = 2^3 - 1 = 7 = 2 \cdot 3 \cdot 1 + 1 = 2 \cdot c_1 \cdot 1 + 1 \equiv 1 \pmod{2c_1}, \\ c_3 &= 2^{c_2} - 1 = 2^7 - 1 = 127 = 2 \cdot 3^2 \cdot 7 \cdot 1 + 1 = 2 \cdot c_1^2 \cdot c_2 \cdot 1 + 1 \equiv 1 \pmod{2c_1^2 c_2}, \\ c_4 &= 2^{c_3} - 1 = 2^{127} - 1 = 170141183460469231731687303715884105726 + 1 \\ &= 2 \cdot 3^3 \cdot 7^2 \cdot 127 \cdot 19 \cdot 43 \cdot 73 \cdot 337 \cdot 5419 \cdot 92737 \cdot 649657 \cdot 77158673929 + 1 \\ &= 2 \cdot c_1^3 \cdot c_2^2 \cdot c_3 \cdot m_3 + 1 \equiv 1 \pmod{2c_1^3 c_2^2 c_3}. \end{aligned}$$

We note that $c_5 = 2^{2^{127}-1} - 1 > 10^{5121759971936968187500605462505161634 9}$. Thus $c_5 - 1$ is too huge to find its prime factorization. However, Theorem 2.5 tells us that

$$\begin{aligned} c_5 &\equiv 1 \pmod{2c_1^4c_2^3c_3^2c_4} \\ &\equiv 1 \pmod{2 \cdot 3^4 \cdot 7^3 \cdot 127^2 \cdot 170141183460469231731687303715884105727}. \end{aligned}$$

Remark 2.7 : Let us consider the Mersenne number $2^5 - 1 = 31$ which is a prime. It is well-known that

$$2^{2^5-1} - 1 = 2^{31} - 1 = 2147483647$$

is also a Mersenne prime. However, one can check that

$$\begin{aligned} 2^{2^5-1} - 1 = 2^{31} - 1 = 2147483647 &\equiv 1 \pmod{31} \\ &\equiv 22 \not\equiv 1 \pmod{5^2}. \end{aligned}$$

Hence the congruence (4) does not hold in general.

REFERENCES

1. L. E. Dickson, *History of the theory of numbers, Vol. 1: Divisibility and primality*, New York, Dover (2005).
2. D. H. Lehmer, An extended theory of Lucas' functions, *Ann. of Math. (2)*, **31**(3) (1930), 419-448.
3. É. Lucas, Théorie des fonctions numériques simplement périodiques, *Amer. J. Math.*, **1** (1878), 184-240, 289-321.
4. K. H. Rosen, *Elementary number theory and its applications*, sixth edition, Pearson Addison Wesley (2011).