2011년 8월
교육학석사(수학교육)학위논문

메르센느 수에 관하여

조선대학교 교육대학원

수학교육전공

김 진 화

[UCI]I804:24011-200000241937

메르센느 수에 관하여

A study of Mersenne Number.

2011 년 8 월

조선대학교 교육대학원

수학교육전공

김 진 화

메르센느 수에 관하여

지도교수 박 순 철

이 논문을 교육학석사학위 청구논문으로 제출합니다.

2011 년 4 월

조선대학교 교육대학원

수학교육전공

김 진 화

김진화의 교육학 석사학위 논문을 인준함.

심사위원장 조선대학교 교수 한 승 국 인

심사위원 조선대학교 교수 박 순 철 인

심사위원 조선대학교 교수 안 영 준 인

2011 년 6 월

조선대학교 교육대학원

목　　차

◎ Abstract

Ⅰ. 서　　론 ····· 1

Ⅱ. 기초 정수론 ····· 4

Ⅲ. 메르센느 수 ····· 17

1. 메르센느의 생애 ····· 17

2. 메르센느 수와 관련된 성질들 ····· 19

1) 메르센느 수의 기본 성질 ····· 19

2) 메르센느 수와 완전수의 관계 ····· 26

3. 메르센느 소수 찾기 ····· 33

1) 전자 컴퓨터 시대 이전 ····· 33

2) 전자 컴퓨터 시대 이후 ····· 35

4. 메르센느 소수 판정 ····· 39

1) 루카스 - 레머 판정법 ····· 39

2) GIMPS와 PrimeNet ····· 43

5. 메르센느 수와 미해결 문제들 ····· 47

1) 메르센느의 소수와 합성수는 무한히 많을까? ····· 47

2) 홀수 완전수는 존재하는가? ····· 49

◎ 참 고 문 헌 ····· 51

ABSTRACT

A study of Mersenne Number.

Kim Jin-hwa

Advisor : Prof. Park Soon-cheol, Ph. D.

Major in Mathematics Education

Graduate School of Education, Chosun University

Doing research on a number has become a study project for a lot of mathematicians since the start of the Pythagoras School in Greece in 300 BC. Especially, since Euclid proved the fundamental theorem of arithmetic, a prime has been playing a great role in the research on the number theory.

Amongst all, a lot of mathematicians have conducted the research work on the numbers of having a special form, and Mersenne's prime belongs to one of them.

The Mersenne's number having the form like $M_n = 2^n - 1$ when n is an integer is called Mersenne prime when M_p is a prime(p is a prime). Such

Mersenne number is called so by adding the name of the 17th century mathematician Marin Mersenne, and due to its special form, it is used for modern cryptology and performance test of the computer; in addition, the Mersenne number is also the biggest form of a prime ever known up to the present.

Accordingly, in Chapter II of this thesis, this research is going to delve into the Mersenne number more deeply after doing explanation about the contents of the basic number theory needed for the understanding of the properties of a number.

In Chapter III, this research intends to look at the judging method for finding the Mersenne numbers after looking at the definition of the Mersenne number through Mersenne's life and also looking at the process of finding the Mersenne prime together with the general properties of Mersenne's numbers. In addition, this research introduces the unsolved problems with the Mersenne numbers.

Ⅰ. 서 론

김승욱(2009)에 따르면 고대 그리스의 피타고라스학파는 우주의 근본적인 구성원소를 밝히는 것을 추구하였는데 그 과정에서 수학이 일정 부분을 차지하였고 그 중에서도 특히 정수가 핵심적인 역할을 하였다고 한다. 피타고라스학파에서 숫자들은 수학적 크기만을 의미하는 것이 아니라 수학적인 상징과도 같았다. 또한 피타고라스학파는 가장 현명한 것이 무엇인가에 대한 질문의 답이 숫자라고 할 정도로 그들에게 숫자는 신비한 것으로, 심지어 우주의 다양성을 숫자들의 법칙을 통해 볼 수 있다고 생각하였다. [1]

이처럼 피타고라스학파에 의해 수에 대한 연구가 시작된 이후 수에 대한 연구는 2500여 년이 지난 지금까지도 많은 수학자들의 연구과제가 되고 있다. 그 중에서도 유클리드가 1보다 큰 모든 자연수는 소수 또는 소수들의 곱으로 유일하게 표현될 수 있다는 산술의 기본 정리를 증명한 이후 소수는 정수의 성질을 밝히는데 중요한 역할을 하고 있다.

특히, 많은 수학자들은 모든 소수를 어떤 하나의 공식으로 만들기 위해 노력하였는데 아직까지 소수를 하나의 공식화하는 데는 실패했지만 이를 통해 여러 가지 특별한 형태의 수들이 알려지게 되었다.

먼저 페르마 수(Fermat Number)는 $F_n = 2^{2^n} + 1$ 같은 형태의 정수인데 이 F_n이 소수일 때 페르마 소수라고 한다. 페르마는 n이 정수일 때 F_n이 모두 소수라고 주장하였는데 이는 다른 수학자들에 의해 사실이 아님이 밝혀졌다. 사실 $F_5 = 2^{2^5} + 1 = 4294967297$은 합성수이며 $n > 4$이상인 페르마 소수 F_n은 아직 알려지지 않고 있다.

메르센느 수(Mersenne Number)는 프랑스의 신부 마린 메르센느의 이름을 따서 불리는 수로 $M_n = 2^n - 1$과 같은 형태의 수이다. 메르센느 수 M_n이 소수일 때 이를 메르센느 소수라고 한다. 이와 같은 메르센느 수는 완전수와 일대일대응의 관계를 이루고 있다. 완전수는 자기 자신을 제외한 양의 약수의 합이 자기 자신과 같은 수이다.

그리고 쌍둥이 소수는 하나의 식으로 나타내지는 수는 아니나 p와 $p+2$가 모두 소수인 짝을 이루는 소수로서 그 개수가 무한하다고 여겨지는 특별한 수이다. 또한 이러한 수 이외에도 친화수나 삼각수, 사촌 소수나 샴쌍둥이 소수 등 여러 가지 형태의 수들이 있다.

이와 같이 특별한 의미를 갖는 여러 가지 수중에서 본 논문에서는 메르센느 수에 흥미를 가지고 메르센느 수의 성질에 대해 소개하고자 한다. 많은 수들 가운데서도 메르센느 수에 특별히 흥미를 가지는 것은 메르센느 수를 찾으면서 컴퓨터의 성능을 시험하기도 하고 메르센느 소수를 이용하여 암호학 등 많은 분야에 사용되고 있기 때문이다. 또한 메르센느 소수는 바로 지금까지 알려진 소수 중 가장 큰 소수를 기록하고 있기도 하다. 2008년 9월 한국일보의 "1300만 자리 메르센느 소수 발견"이라는 제목의 기사에서 이 소수의 발견에 대한 내용을 찾아볼 수 있다.

"미 로스앤젤레스 캘리포니아대(UCLA)의 수학자들이 지금까지 확인된 것으로는 최대인 1,300만 자리 '소수'를 발견했다고 AP통신이 27일 보도했다.

UCLA 수학자 팀은 윈도우XP를 탑재한 75대의 네트워크 컴퓨터를 통해 지난달 최대 숫자인 '메르센느 소수'를 발견했으며, 다른 연산을 사용하는 컴퓨터 시스템으로 이 소수의 존재를 검증했다.

소수는 3, 7, 11처럼 그 자신의 수와 1로만 나눠지는 수로, 이번에 발견된 메르센느 소수는 '$2^{42112609} - 1$'이다. 17세기 프랑스 수학자 마린 메르센느의 이름을 딴 메르센느 소수는 메르센느가 2의 제곱인 수에서 1을 뺀 수중에 소수가 많다는 점에

착안해 만들어진 소수다. 즉 '2^n-1'인 숫자 중 소수가 되는 경우를 지칭한다.

UCLA 수학자팀 리더인 에드슨 스미스는 '숫자가 커질수록 소수를 찾을 확률은 급격히 낮아지지만, 우리는 더 큰 소수를 찾고 있다'고 말했다. '전자선구자 재단(EEF)'이 주관하는 '인터넷 메르센느 소수 찾기' 프로젝트인 GIMPS(Great Internet Mersenne Prime Search)에는 현재 전 세계 수천 명이 참가하고 있으며 1,000만 이상 자리의 소수를 발견하는 사람에게는 10만 달러의 상금을 지급한다." [18]

그리하여 본 논문에서는 마린 메르센느(Marin Mersenne)의 생애와 메르센느 수의 기본 성질을 살펴보고 메르센느 소수를 찾는 역사와 함께 최근까지 알려진 메르센느 소수에 대해 알아본 후 메르센느 소수를 쉽게 찾기 위한 판정법을 살펴보고자 한다. 또한 아직까지 메르센느 수와 관련하여 풀리지 못한 가설들에 대해 소개하고 메르센느 소수를 찾기 위한 GIMPS 프로젝트의 prime95 프로그램을 통해 직접 간단한 메르센느 소수를 찾아보고자 한다.

Ⅱ. 기초 정수론

• 합동식

두 정수 a, d에 대해

$$a = de$$

인 정수 e가 존재할 때, d를 a의 약수(divisor) 또는 인수(factor)라고 하고 a를 d의 배수(multiple)이라고 한다. 이를 $d|a$로 나타낸다.

또한 두 정수 a, b에 대해 a와 b에 공통으로 약수가 되는 정수 e가 존재할 때 그 정수 e를 a, b의 공약수(common divisor)라 한다. 그리고 다음 세 조건을 만족하는 정수 d를 a와 b의 최대공약수(greatest common divisor)라 하고 이를 $(a, b) = d$로 나타낸다.

(ⅰ) $d \geq 0$

(ⅱ) $d|a$, $d|b$

(ⅲ) 정수 e에 대해 e가 a와 b의 공약수이면 $e|d$이다.

만약 a와 b의 최대공약수가 1이면 두 정수 a, b는 서로소(relatively prime)라고 한다.

정의 2.1

양의 정수 m과 정수 a, b에 대해

$$m|(a-b)$$

일 때, a와 b는 법(modulus) m에 관하여 합동(congruent)이라 하고 이를 $a \equiv b \pmod{m}$이라고 나타낸다. 즉,

$$m|(a-b) \Leftrightarrow a \equiv b \pmod{m}$$

이다. 또한 a와 b가 법 m에 관하여 합동이 아닐 때 $a \not\equiv b \pmod{m}$이라고 나타낸다.

정리 2.1

양의 정수 m과 임의의 정수 a, b, c, d에 대해 다음이 성립한다.

(1) $a \equiv a \pmod{m}$

(2) $a \equiv b \pmod{m}$이면 $b \equiv a \pmod{m}$이다.

(3) $a \equiv b \pmod{m}, b \equiv c \pmod{m}$이면 $a \equiv c \pmod{m}$이다.

(4) $a \equiv b \pmod{m}, c \equiv d \pmod{m}$이면 $a \pm c \equiv b \pm d \pmod{m}$, $ac \equiv bd \pmod{m}$ 이다.

(증명)

(1) $m|(a-a)$이므로 $a \equiv a \pmod{m}$이다.

(2) $a \equiv b \pmod{m}$이면 $m|(a-b)$이고 이는 $m|(b-a)$이므로 $b \equiv a \pmod{m}$이다.

(3) $a \equiv b \pmod{m}, b \equiv c \pmod{m}$이면 $m|(a-b), m|(b-c)$이다. 이 때,

$$a-c=(a-b)+(b-c)$$

이므로 $m|(a-c)$가 되어 결국 $a \equiv c \pmod{m}$이다.

(4) 합동의 정의에 의해

$$a \equiv b \pmod{m} \Leftrightarrow m|(a-b),\ c \equiv d \pmod{m} \Leftrightarrow m|(c-d)$$

가 되고

$$(a \pm c)-(b \pm d)=(a-b) \pm (c-d),$$

$$ac-bd=(a-b)c+b(c-d)$$

이므로

$$m|\{(a \pm c)-(b \pm d)\},\ m|(ac-bd)$$

를 만족한다.

그러므로 $a \pm c \equiv b \pm d \pmod{m}$, $ac \equiv bd \pmod{m}$이다. □

정리 2.2

양의 정수 m과 임의의 정수 a에 대해 a를 m으로 나누었을 때의 나머지를 r이라고 하면

$$a \equiv r \pmod{m}, \qquad o \le r < m$$

이다. 그리고 법 m에 관하여 0, 1, $\cdots$, $m-1$은 어느 둘도 합동이 아니다.

(증명)

나눗셈 정리에 의해

$$a = mq + r, \qquad 0 \le r < m$$

인 정수 q, r이 존재하고 이 때 $a \equiv r \pmod{m}$, $0 \le r < m$이다.

또한 $0 \le r < m$, $0 \le s < m$인 두 정수 r, s에 대해 $r \equiv s \pmod{m}$이라고 하면

$$r \equiv s \pmod{m} \Leftrightarrow m \mid (r-s)$$

이고 $-m < r-s < m$이므로 $r-s=0$이 되어 결국 $r=s$이다.

따라서 법 m에 관하여 0, 1, $\cdots$, $m-1$ 중 어느 둘도 합동이 아니다.

□

정리 2.3 페르마의 소 정리(Fermat's little theorem).

소수 p에 대하여 다음이 성립한다.

(1) 모든 정수 a에 대해 $a^p \equiv a \pmod{p}$이다.

(2) $(a,p)=1$인 정수 a에 대하여 $a^{p-1} \equiv 1 \pmod{p}$이다.

(증명)

(1) 임의의 두 정수 a, b에 대해

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \cdots + \binom{p}{r}a^{p-r}b^r + \cdots + b^p$$

이다. 이 때, $\binom{p}{r} = \dfrac{p!}{r!(p-r)!}$은 정수이다.

$1 \le r \le p-1$일 때 $p \nmid 1 \cdot 2 \cdots \cdot r$, $p \nmid 1 \cdot 2 \cdots \cdot (p-r)$이지만 $p \mid p!$이므로

$$p \mid \binom{p}{r} \Leftrightarrow \binom{p}{r} \equiv 0 \pmod{p}$$

이다. 따라서

$$(a+b)^p \equiv a^p + b^p \pmod{p}$$

가 된다.

(ⅰ) $n=1$일 때, $n \equiv 1^p \equiv 1 = n \pmod{p}$이다.

(ⅱ) 양의 정수 $n=k$에 대해 $k^p \equiv k \pmod{p}$라 하면 $n=k+1$일 때,

$$(k+1)^p \equiv k^p + 1^p \equiv k+1 \pmod{p}$$

가 되어 모든 양의 정수 n에 대하여 $n^p \equiv n \pmod{p}$이다.

또한 $0^p \equiv 0 \pmod{p}$이고 양의 정수 n에 대해 소수 p가 짝수($p=2$)이면

$$(-n)^p \equiv n^p \equiv n \equiv -n \pmod{p}$$

이고 p가 홀수 소수이면

$$(-n)^p \equiv -n^p \equiv -n \pmod{p}$$

가 된다.

그러므로 모든 정수 a에 대해 $a^p \equiv a \pmod{p}$이다.

(2) (1)에 의해 모든 정수 a에 대해 $a^p \equiv a \pmod{p}$이므로 $(a,p)=1$일 때 $a^{p-1} \equiv 1 \pmod{p}$가 된다.

□

• 소수

소수(Prime)란 2보다 크거나 같은 정수로써 양의 약수가 1과 자기 자신 뿐인 수를 말한다. 또한 소수가 아닌 정수를 합성수(composite number)라고 한다. 즉, 정수 d와 e가 존재하여

$$a = de \qquad (1 < d, e < a)$$

일 때 정수 a가 합성수이다. 그리고 정수 a의 약수 중에서 소수인 약수를 a의 소인수(Prime factor)라고 한다.

정수 p, q가 소수일 때, 정수 a, b와 m, $n(m, n \geq 1)$에 대해

(1) $p|a \Leftrightarrow (a,p) = p, \quad p \nmid a \Leftrightarrow (a,p) = 1$

(2) $(a, p^n) = 1 \Leftrightarrow (a, p) = 1 \Leftrightarrow p \nmid a$

(3) $(p, q) = 1 \Leftrightarrow (p^m, q^n)$

(4) $p|ab$이면 $p|a$ 또는 $p|b$

와 같은 성질을 만족한다. 이에 대한 증명은 참고문헌 [2]를 참조하면 된다.

정리 2.4

2보다 크거나 같은 정수 a에 대해 a의 소인수가 적어도 하나 존재한다.

(증명)

정수 a의 약수 중 2 이상인 약수 전체의 집합을 S라 하자.

먼저 $a|a$이고 $a \geq 2$이므로 $S \neq \varnothing$이다. 그러므로 정수의 정렬성에 의해 S에 속하는 정수 중 최소원 $p(\geq 2)$가 존재한다.

이 때, d를 $d|p$, $d \geq 2$인 정수라 하면 $d|p$이고 $p|a$이므로 결국 $d|a$가 되어 p의 최소성에 모순이다.

그러므로 $d=p$이다. 따라서 p는 소수이고 p는 a의 소인수이다.

□

유클리드(Euclidean)는 B. C 350년 경 자신의 저서인 기하학원론에서 '소수가 무한히 많다.' 라는 정리를 증명하였다. 또한 그는 임의의 양의 정수는 그 자체로 소수이거나 소수들의 곱으로 표현될 수 있다고 하였다. 그리고 그 표현방법은 오직 하나라는 것을 증명하였다. 즉, 임의의 양의 정수는 유일한 소인수분해를 가진다는 것이다.

소인수분해(prime factorization)란 2보다 크거나 같은 정수 n이 유한 개의 소수 p_1, p_2, $\cdots$, p_t의 곱으로 나타내어질 때 즉,

$$n=p_1p_2\cdots p_t$$

일 때 n은 소인수분해 된다고 한다. 그리고 이 식을 n의 소인수분해라고 한다. 이 때, n의 소인수분해는 단 한가지이다.

정리 2.5

소수는 무수히 많다.

(증명)

소수가 유한개라고 가정하자. 즉, n개의 소수 p_1, p_2, $\cdots$, p_n 만이 존재한다고 할 때 정수 N을

$$N=p_1p_2\cdots p_n+1$$

이라 하면 $N\geq 2$이므로 위의 정리 2.4에 의해 소인수가 적어도 하나 존재하므로 $p|N$인 p가 존재하게 된다. 또한 p는 소수이므로 p_1, p_2, $\cdots$, p_n 중의 어느 하나와 같게 되므로 $p|p_1p_2\cdots p_n$가 된다. 즉, $p|N$, $p|p_1p_2\cdots p_n$이므로 $p|(N-p_1p_2\cdots p_n)$가 되고 이는 곧 $p|1$이므로 모순이다.

따라서 소수는 무수히 많다.

□

정리 2.6

양의 정수 n이 합성수라고 하면, n의 소인수 중에 $p \le [\sqrt{n}]$인 소인수 p가 존재한다.

(증명)

n이 합성수이면 적당한 정수 d, e에 의해

$$n = de, \quad 2 \le d \le e < n$$

이다. 이 때,

$$2^2 \le d^2 \le de = n$$

이므로

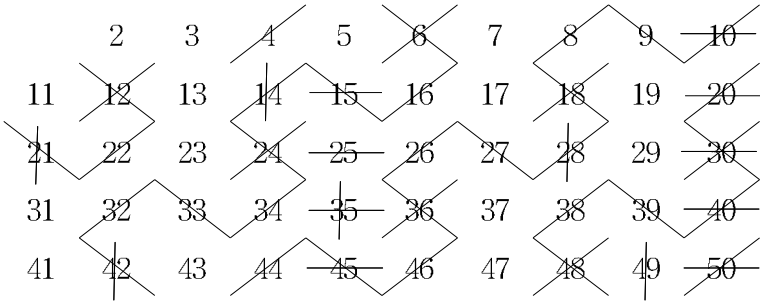
$$2 \le d \le [\sqrt{n}]$$

이다. 그런데 $d \ge 2$이므로 d의 소인수 p가 존재하고 $p|d$, $d|n$이므로 $p|n$이다. 또한 $p \le d$이므로 결국 $p \le [\sqrt{n}]$이 된다.

□

예를 들어, 50이하의 소수를 찾아보자. $[\sqrt{50}] = 7$이므로 7보다 작거나 같은 소수는 2, 3, 5, 7뿐이다. 그러므로 50이하의 정수 중 소수는 2, 3, 5, 7의 배수가 아닌 수들이다. 따라서 50이하의 소수는 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47이 된다. 이와 같이 소수를 찾는 방법을 에라토스테네스(Eratosthenes)[1]의 체라고 한다. 다음 그림을 통해 에라토스테네스의 체에 대해 자세히 알 수 있다.

1) 에라토스테네스(Eratosthenes). B. C 200년경 고대 그리스의 수학자. 소수를 발견하는 방법으로 에라토스테네스의 체를 고안하고, 해시계로 지구 둘레의 길이를 처음으로 계산하였다.



이제 $4n+1$형태의 정수들의 곱을 살펴보자. $k_1 = 4m+1$, $k_2 = 4n+1$이라 하면

$$\begin{aligned} k_1 k_2 &= (4m+1)(4n+1) \\ &= 16mn + 4m + 4n + 1 \\ &= 4(4mn + m + n) + 1 \end{aligned}$$

이 되어 결국 $4n+1$과 같은 형태가 된다. 그러므로 $4n+1$형태의 정수들의 곱은 항상 같은 형태가 됨을 알 수 있다.

정리 2.7

$4n+3$ 형태의 소수는 무수히 많다.

(증명)

$4n+3$형태의 소수가 유한개라고 가정하자. 이 소수들을

$$p_1,\ p_2,\ \cdots,\ p_s$$

라 하고 N을

$$N = 4p_1p_2 \cdots p_s - 1 = 4(p_1p_2 \cdots p_s - 1) + 3$$

이고 $N = r_1 r_2 \cdots r_t$으로 소인수분해 된다고 하자. 이때, N은 홀수이므로 $r_k\,(1 \le k \le t)$은 $4n+1$ 또는 $4n+3$의 형태이다. 그런데 $4n+1$ 형태의 정수들의 곱은 같은 형태를 가지므로 적어도 하나의 소수r_k는 $4n+3$의 형태가 된다. 따라서

$$r_k | N+1,\ r_k | N$$

이므로 $r_k|1$이 되는데 이는 r_k가 소수라는 사실에 모순이다.

따라서 $4n+3$과 같은 형태의 소수는 무수히 많다.

□

정리 2.8

$4n+1$형태의 소수는 무수히 많다.

(증명)

$4n+1$형태의 소수가 유한개 존재한다고 가정하자. 이 때 이러한 소수를

$$p_1,\ p_2,\ \cdots,\ p_n$$

이라고 하자. 이 때

$$N=(2p_1p_2\cdots p_n)^2+1$$

이라 하면 N은 홀수이고 $N\geq 2$이므로 $p|N$인 홀수 p가 존재하여

$$(2p_1p_2\cdots p_n)^2\equiv(-1)\pmod p$$

$$\Leftrightarrow 4p_1^2p_2^2\cdots p_n^2\equiv(-1)\pmod p$$

이다. 즉, p는 $4n+1$ 형태의 소수가 되어 $p_1,\ p_2,\ \cdots,\ p_n$ 중 어느 하나와 일치한다. 그러므로 $p|p_1p_2\cdots p_n$이다. 그런데 앞에서 $p|N$라 하였으므로 결국

$$p|N-(2p_1p_2\cdots p_n)^2$$

으로 $p|1$이 되어 모순이 생긴다.

따라서 $4n+1$ 형태의 소수는 무수히 많다.

□

프랑스의 수학자인 디리클레(Dirichlet)는 디리클레 급수를 이용하여 정수 a와 b가 서로소일 때, $an+b$ 형태의 소수는 무수히 많다는 것을 증명하였다.

• 위수

정수 $m(m \geq 2)$과 서로소인 정수 a에 대해

$$a^k \equiv 1 \pmod{m}$$

인 가장 작은 양의 정수 k을 법 m에 관한 a의 위수라 하고 $k = \mathrm{ord}_m a$로 나타낸다.

정리 2.9

정수 a의 법 m에 관한 위수를 k라 하자. $k|h$인 필요충분조건은 $a^h \equiv 1 \pmod{m}$이다.

(증명)

$k|h$이므로 정수 r가 존재하여 $h = kr$로 나타낼 수 있다. 이 때, $a^k \equiv 1 \pmod{m}$이므로 $a^{kr} \equiv 1 \pmod{m}$이고 결국 $a^h \equiv 1 \pmod{m}$이 된다.

역으로 $a^h \equiv 1 \pmod{m}$이라 하자. 나눗셈 정리에 의하면 적당한 정수 q, r이 존재하여 $h = qk + r$ $(0 \leq r < k)$가 되므로

$$1 \equiv a^h = a^{qk+r} = a^{qk}a^r \pmod{m}$$

이다. 이 때, k가 법 m에 관한 a의 위수이므로 $a^k \equiv 1 \pmod{m}$이다. 따라서

$$a^{qk}a^r \equiv a^r \equiv 1 \pmod{m}$$

이 되고 $0 \leq r < k$이므로 $r = 0$이다. 결국 $h = qk$가 되어 $k|h$이다.

□

• 르장드르기호

정수 $m(m \geq 3)$과 $(a, m) = 1$인 정수 a에 대하여 법 m에 관한 이차 합동식

$$x^2 \equiv a \pmod{m}, \quad (a, m) = 1$$

의 해가 존재할 때, 즉 $c^2 \equiv a \pmod{m}$인 정수 c가 존재하는 경우에 a를 법 m에 관한 이차잉여(quadratic residue)라고 한다.

또한 위 식의 해가 존재하지 않을 때 a를 법 m에 관한 이차비잉여(quadratic nonresidue)라 한다.

정의 2.3

홀수인 소수 p와 $(a, p) = 1$인 정수 a에 대해 르장드르(Legendre)기호 $\left(\frac{a}{p}\right)$의 값을 다음과 같이 정의한다.

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & (a\text{가 법 } p\text{에 관한 이차잉여일 때}) \\ -1, & (a\text{가 법 } p\text{에 관한 이차비잉여일 때}) \end{cases}$$

정리 2.10

홀수 소수 p와 $(a, p) = (b, p) = 1$인 정수 a, b에 대하여 다음이 성립한다.

(1) $\left(\frac{a^2}{p}\right) = 1, \quad \left(\frac{1}{p}\right) = 1$

(2) $a \equiv b \pmod{p}$이면 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$이다.

(3) $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$

(4) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(증명)

(1) 이차합동식 $x^2 \equiv a^2 \pmod{p}$는 두 개의 해 $x \equiv \pm a \pmod{p}$를 가지므로 $\left(\frac{a^2}{p}\right) = 1$ 이다.

(2) $a \equiv b \pmod{p}$이면 두 이차합동식 $x^2 \equiv a \pmod{p}$와 $x^2 \equiv b \pmod{p}$는 서로 동치이므로 $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$이다.

(3) a가 p의 이차잉여류 또는 이차비잉여류라는 것은

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \text{ 또는 } a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

에 의해 결정된다. 그러므로 이를 르장드르 기호로 나타내면 $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$이다.

(4) (3)에 의해 $\left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod{p}$이다. 한편 이 식의 좌변과 우변의 값은 1 또는 -1 이고 p는 홀수 소수이므로 $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$이다.

□

정리 2.11

서로 다른 홀수 소수 p, q에 대해 다음이 성립한다.

(1) $\left(\frac{2}{p}\right) = 1 \Leftrightarrow p \equiv \pm 1 \pmod{8}$

$\left(\frac{2}{p}\right) = -1 \Leftrightarrow p \equiv \pm 3 \pmod{8}$

(2) $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right) \Leftrightarrow p \equiv 1 \pmod{4}$ 또는 $q \equiv 1 \pmod{4}$

$\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right) \Leftrightarrow p \equiv q \equiv 3 \equiv -1 \pmod{4}$

(증명)

(1) 홀수 소수 p는 $8k \pm 1$ 또는 $8k \pm 3$의 꼴이다. 이 때,

$p = 8k \pm 1$이면 $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{2(4k^2 \pm k)} = 1$이고

$p = 8k \pm 3$이면 $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{2(4k^2 \pm 3k)+1} = -1$이다.

그러므로 (1)이 성립한다.

(2) p, q는 홀수이므로 $p \equiv \pm 1 \pmod 4$, $q \equiv \pm 1 \pmod 4$이다. 이 때,

$p \equiv 1 \pmod 4$ 또는 $q \equiv 1 \pmod 4$이면 $\frac{p-1}{2}\frac{q-1}{2}$는 짝수이고

$p \equiv q \equiv -1 \equiv 3 \pmod 4$이면 $\frac{p-1}{2}\frac{q-1}{2}$는 홀수이다.

그러므로 (2)가 성립한다.

□

Ⅲ. 메르센느 수

1. 메르센느의 생애

마린 메르센느(Marin Mersenne. 1588-1648)는 1588년 9월 8일 프랑스 메인(Maine)주의 오이제(Oize)라는 작은 마을에서 태어났다. 문법 수업을 위해 망스학교(College of Mans)를 다닌 후 16살이 되던 1604년에 8살이나 어렸던 데카르트와 함께 라 플레쉐(La Fleche)의 제수이트 학교(College Jesuit)에 입학했다.

5년간 제수이트 학교에서 공부한 뒤 1609년부터 1611년까지 소르본(Sorbonne)에서 신학을 배워 1612년에 신부가 되었다. 또한 그는 1611년 '미님스(Minims)'[2]라는 종교 단체에 가입하였고 1614년부터 1618년까지 미님스의 수도원에서 철학을 강의하기도 하였다.

메르센느는 철학과 함께 수학, 과학에 흥미가 있었다. 그는 당시에 많은 신학자들에게 비판을 받고 있었던 데카르트(Descartes)와 갈릴레오(Galileo)를 옹호하였으며 최초의 단진자 시계를 발명한 호이겐스(Huygens)에게 단진자 사용을 제안하기도 했다. 그리고 그는 음악에도 큰 관심을 갖고 있어서 화음에 관한 최초의 이론을 개발하기도 하였다.

또한 그는 유럽 전역에 있는 수학자와 철학자 사이를 잇는 역할을 했다. 그는 수많은 학자들과 서신을 주고받았으며 파리에 있던 그의 집에서 페르마와 파스칼 등의 학자들과 만나기도 하였다. 1648년 9월 1일 그가 세상을 떠난 후 그의 방에서는

2) 미님스(Minims). 최소를 의미하는 Minimi에서 유래. 1436년 성 프란시스(St Francis)에 의해 설립된 종교단체로 그들 자신들이 모든 종교적인 것들의 근본이 되고자 하였다. 그들은 지구상의 모든 종교 중에서 자신들이 가장 마지막이라고 믿었으며 기도와 신학 공부에 헌신하였다. 프랑스혁명 이후 그 수가 줄어들어 현재 이탈리아에 몇 개의 수도원만 존재하고 있다.

토리첼리(torricelli)와 데카르트, 파스칼과 그의 부친을 비롯한 많은 학자들과 주고받은 서신이 78통이나 발견되었으며 이는 수학사 연구에 큰 도움이 되었다. 그 중 1640년 크리스마스에 페르마가 메르센느에게 보낸 서신을 보면 어떤 소수는 두 제곱수의 합으로 쓸 수 있다는 자신의 발견에 대한 내용이 쓰여 있다. 이렇게 많은 학자들과 수학적인 발견을 공유하면서 그는 학술잡지가 없던 당시에 유럽 전역의 많은 수학자들 사이에서 국제적 과학 정보센터와 같은 역할을 수행하였다.

수학은 메르센느가 가장 깊게 연구했던 분야였으며 그는 수학 없이 어떤 과학도 가능하지 못하다고 믿었다. 메르센느는 수학을 순수하게 지적인 상상력의 과학이라고 주장하면서 수학은 수량을 확실하게 다루기 때문에 절대적으로 가능한 것 이외에는 어떤 것도 고려하지 않는다고 하였다. 그는 특히 소수에 대해 큰 관심을 갖고 모든 소수를 표현하는 식을 찾는 것에 대해 연구하였다. 그리하여 마침내 1644년 그의 저서인 《물리수학론(Cogitata Physica-Mathematica)》를 통해

"$n \le 257$일 때, n이 2, 3, 5, 7, 13, 19, 31, 67, 127, 257이라면 $2^n - 1$은 소수가 된다."

라는 주장을 하였다. 이 주장은 후에 다른 사람들에 의해 사실이 아님이 밝혀졌지만 $2^n - 1$과 같은 형태의 수는 아직까지도 많은 수학자들의 연구 과제가 되고 있다. 우리는 이러한 메르센느의 업적을 기리면서 $2^n - 1$과 같은 형태의 수를 메르센느 수라고 부른다.

정의 3.1 메르센느 수(Mersenne Number).

n이 2보다 큰 정수일 때, $M_n = 2^n - 1$과 같은 수를 메르센느 수(Mersenne Number)라고 한다. 특히, p가 소수일 때

$$M_p = 2^p - 1$$

가 소수이면 $M_p = 2^p - 1$을 메르센느 소수(Mersenne Prime)라고 한다.

2. 메르센느 수와 관련된 성질들

1) 메르센느 수의 기본 성질

우리는 앞에서 메르센느 수 $M_n = 2^n - 1$에 대해 알았다. 그런데 p가 소수일 때, $M_p = 2^p - 1$가 모두 소수가 되는 것은 아니다.

예를 들어 $p = 3$일 때, $M_3 = 2^3 - 1 = 7$은 소수이다. 그러나 $p = 11$는 소수이지만 $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$은 소수가 아니다.

그러나 그 역은 성립한다는 것을 다음 정리를 통해 알 수 있다.

정리 3.1

메르센느 수 $M_n = 2^n - 1$이 소수이면, n은 소수이다.

(증명)

(i) $n = 1$일 때,

$$M_1 = 2^1 - 1 = 1$$

이므로 M_1은 소수가 아니다.

(ii) n이 합성수라고 가정하자. 그러면 n은 1보다 큰 정수 a와 b의 곱으로 나타내어질 수 있다. 즉, $n = ab\ (a > 1, b > 1)$이다.

이를 $M_n = 2^n - 1$에 대입하여 정리하면

$$\begin{aligned} M_n = 2^n - 1 &= 2^{ab} - 1 \\ &= (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1) \end{aligned}$$

이 되고, $a > 1$, $b > 1$이므로 $2^a - 1 > 1$, $2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1 > 1$이다. 따라서 $M_n = 2^n - 1$은 1보다 큰 두 정수의 합성수가 된다.

그러므로 $M_n = 2^n - 1$이 소수이면 n도 소수이다.

□

정리 3.1을 좀 더 확장해서 a가 0보다 크고 n이 2보다 크거나 같은 양의 정수일 때 $a^n - 1$이 소수라고 생각해 보자. $a^n - 1$은

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$$

과 같이 나타낼 수 있다. 이 때 $a^n - 1$이 소수라고 하면

$$a - 1 = 1 \text{ 또는 } a^{n-1} + a^{n-2} + \cdots + a + 1 = 1$$

이 된다. 그런데 $a > 0$, $n \geq 2$인 양의 정수이면 결국

$$a^{n-1} + a^{n-2} + \cdots + a + 1 > 1$$

이 되므로 $a - 1 = 1$이 되어 $a = 2$가 된다. 그런데 이 때, $a = 2$라는 것은 $2^n - 1$이 소수라는 것과 같으므로 정리 3.1에 의해 n도 또한 소수임을 알 수 있다. 즉, $a^n - 1$이 소수이면 $a = 2$가 되고 n은 소수가 된다.

메르센느 수가 특별히 관심 받는 이유는 그 표현방법이 쉽기 때문이다. 특히 메르센느 수 $M_n = 2^n - 1$을 이진법으로 나타내면 n자리 수로 모든 자리의 숫자가 1로만 표현된다. 즉,

$$M_2 = 2^2 - 1 = 3 = 11_{(2)}$$

$$M_5 = 2^5 - 1 = 31 = 11111_{(2)}$$

$$M_7 = 2^7 - 1 = 111111_{(2)}$$

$$M_n = 2^n - 1 = \underbrace{111 \cdots 11}_{n\text{개}}{}_{(2)}$$

과 같다. 이와 같이 메르센느 수를 특별한 형태의 이진법으로 나타내어 보는 것으로 메르센느 수의 약수를 쉽게 찾아낼 수도 있다.

위의 정리 3.1로부터 n이 소수일 때, M_n이 소수일수도 그렇지 않을 수도 있다는 것을 알았다. 이제 메르센느 수의 약수와 배수에 대해 알아보도록 하자.

정리 3.2

다음이 성립한다.

(1) $M_m | M_n$이면 $m | n$이다.

(2) p가 소수일 때, $1 < q < p$인 정수 q에 대해 $M_q \nmid M_p$이다.

(3) 소수 p의 배수 중에서 가장 작은 메르센느 수를 M_k라 할 때, p의 배수 중 다른 메르센느 수는 M_k의 배수이다.

(증명)

(1) $m \nmid n$이라고 가정하자.

그러면 적당한 정수 q, $r(0 < r < m)$에 대해 $n = mq + r$이라 할 수 있다. 따라서

$$\begin{aligned} M_n = 2^n - 1 &= 2^{mq+r} - 1 \\ &= (2^{mq+r} - 2^r) + (2^r - 1) \\ &= (2^m - 1)\{2^{m(q-1)+r} + 2^{m(q-2)+r} + \cdots + 2^{m+r} + 2^r\} + (2^r - 1) \\ &= (\sum_{k=0}^{q-1} 2^{km+r}) \times (2^m - 1) + (2^r - 1) \\ &= (\sum_{k=0}^{q-1} 2^{km+r}) \times M_m + M_r \end{aligned}$$

이다. 이 때, $0 < r < m$이므로 $0 < M_r < M_m$이 된다.

그러므로 $M_m \nmid M_n$이 된다.

(2) p가 소수이면 $0 < q < p$인 q는 p의 약수가 될 수 없다. 따라서 (1)에 의해 $M_q = 2^q - 1$ $(1 < q < p)$는 M_p의 약수가 아니다.

(3) p의 배수 M_n에 대해 $M_k \nmid M_n$이라고 가정하자. 나머지 정리에 의하여

$$M_n = M_k \times (2^{r+1} + 2^{k+r+1} + 2^{2k+r+1} + \cdots + 2^{(q-1)k+r+1}) + M_r \ , \quad (o < r < k)$$

인 정수 q, r이 유일하게 존재한다. 여기서 좌변의 M_n은 p의 배수이므로 위 식의 우변 또한 p의 배수가 된다. 그런데 이것은 k의 최소성에 모순이 된다.

따라서 M_n은 M_k의 배수이다.

□

정리 3.3

p와 $q=2p+1$이 소수일 때, 다음 중 어느 하나만 성립한다.

(1) $q|M_p$

(2) $q|(M_p+2)$

(증명)

정리 2.3의 페르마의 소정리를 이용하여 증명한다.

$q=2p+1$이 소수이므로

$$2^{q-1}-1 \equiv 0 \pmod{q}$$

이다. 이를 인수분해 하면

$$\begin{aligned} 2^{q-1}-1 &= (2^{\frac{q-1}{2}}-1)(2^{\frac{q-1}{2}}+1) \\ &= (2^p-1)(2^p+1) \equiv 0 \pmod{q} \end{aligned}$$

가 되어 $M_p(M_p+2) \equiv 0 \pmod{q}$이다.

즉, $q|M_p$ 또는 $q|(M_p+2)$이다.

이 때, q가 M_p와 M_p+2를 동시에 나눌 수는 없다.

그러므로 $q|M_p$ 또는 $q|(M_p+2)$ 둘 중에 어느 하나만 성립한다.

□

위의 정리에서 구체적으로 어떤 경우에 $q|M_p$가 되고 어떤 경우에는 $q|(M_p+2)$가 되는지는 다음 정리를 통해 알 수 있다.

정리 3.4

p, $q=2p+1$가 소수일 때, 다음이 성립한다.

(1) $q \equiv \pm 1 \pmod 8$이면 그리고 그 때에만 $q|M_p$이다.

(2) $q \equiv \pm 3 \pmod 8$이면 그리고 그 때에만 $q|(M_p+2)$이다.

(증명)

(1) $q|M_p$는 $2^{\frac{q-1}{2}} = 2^p \equiv 1 \pmod q$와 동치이다. 이는 정리 2.10의 (3)에 의해

$$\left(\frac{2}{p}\right) \equiv 2^{\frac{q-1}{2}} \equiv 1 \pmod p$$

이다. 이 때, 이는 다시 정리 2.11의 (1)에 의해 $p \equiv \pm 1 \pmod 8$과 동치가 됨을 알 수 있다.

(2)번도 마찬가지로 증명할 수 있다.

□

예를 들어 $p=3$일 때와 $p=5$ 일 때를 살펴보도록 하자. 먼저 p가 3이면 q는 $2 \cdot 3+1=7$이고 $M_3=2^3-1=7$이다. 이 때 $7 \equiv (-1) \pmod 8$인데 $7|7$이므로 정리 3.4의 (1)과 같이 $7|M_3$가 됨을 알 수 있다.

또한 소수 p가 5, q가 $2 \cdot 5+1=11$일 때, $M_5=2^5-1=31$이고 $11 \equiv 3 \pmod 8$이다. 이 때 $11|33$이므로 정리 3.4의 (2)와 같이 결국 $11|(M_5+2)$가 된다.

정리 3.5

$p \equiv 3 \pmod 4$인 소수일 때, $q=2p+1$이 소수일 필요충분조건은 $q|M_p$이다.

(증명)

$q=2p+1$을 소수라고 하자. $p \equiv 3 \pmod 4$이므로 적당한 정수 k에 대해 $p=4k+3$이라고 나타낼 수 있다. 이를 $q=2p+1$에 대입하면

$$q = 2p + 1 = 2(4k+3) + 1 = 8k + 7$$

이 되어 $q \equiv (-1) \pmod 8$이다.

따라서 위의 정리 3.4의 (1)에 의해 $q | M_p$가 된다.

역으로, $q | M_p$일 때 $q = 2p+1$을 합성수라고 가정하자. 이 때, $q = 2p+1$의 최소 소인수를 a라고 하면 $a | q$이고, $q | M_p$이므로 $a | M_p$이다.

그러므로 페르마 소 정리에 의해 $2^p \equiv 1 \pmod a$가 된다. 즉, 법 a에 관한 2의 위수는 $a-1$과 p의 약수여야 한다. 그런데 p는 소수이므로 1과 p만을 인수로 가지고 결국 p는 $a-1$을 나누어야 하고 $a > p$이다. $q > a$이고 a가 q의 최소 소인수이므로 a와 다른 인수와의 곱이거나 a의 거듭제곱 형태 등이 될 수 있기 때문에 $q \geq a^2$이고 좌변에 1을 더하면 $q+1 > a^2$이 되어

$$q + 1 = (2p+1) + 1 > a^2 > p^2$$

가 된다. 여기에서 $0 > p^2 - 2p - 2 = (p-1)^2 - 3$을 얻을 수 있는데 이는 $p > 2$에 모순이다. 그러므로 $q = 2p+1$은 소수이다.

□

예를 들어 $p = 7$일 때 $q = 2 \cdot 7 + 1 = 15$는 소수가 아니다. 그러므로 정리에 3.5에 의해 $15 \nmid M_7$이다. 실제로 $M_7 = 2^7 - 1 = 127$으로 $15 \nmid 127$이고 127은 소수이다.

또한 $p = 11$일 때 $q = 2 \cdot 11 - 1 = 23$는 소수이므로 $23 | M_{11}$이 되어 M_{11}이 합성수이고 23이 $M_{11} = 2^{11} - 1 = 2047$의 소인수가 됨을 알 수 있다. 이를 통해 M_{11}의 소인수를 23을 찾을 수 있다. M_{11}의 소인수분해는 $M_{11} = 23 \cdot 89$이며 더 큰 메르센느 수 M_p의 소인수도 위 정리를 통해 쉽게 찾을 수 있다.

정리 3.6

p가 홀수인 소수라고 하면 M_p의 소인수는 $2kp+1$의 형태이다.

(증명)

q가 M_p의 임의의 소인수라고 하자.

즉, $q|M_p$이면 페르마의 소 정리에 의해 $2^p \equiv 1 \pmod{q}$이다. 2가 법 q에 대해 위수가 k라고 하면 결국 $k|p$이다.

그러나 $k=1$이면 $q \nmid 1$이므로 $k \neq 1$이다. 그러므로 $k>1$일 때, $k=p$라고 생각해 보자. 페르마 소 정리에 의해 $2^{q-1} \equiv 1 \pmod{q}$이고 $k|(q-1)$이다. 그리고 $k=p$이므로 결국 $p|(q-1)$이 된다.

그러므로 적당한 t에 대하여 $q-1=pt$라고 할 수 있다. 즉, $q=pt+1$이다. 그런데 만약 t가 홀수가 되면 p도 홀수이므로 $q=pt+1$은 짝수가 되어 가정에 모순이 된다.

따라서 $q=2kp+1$이다.

□

위의 정리 3.6을 확장하여 M_p의 임의의 소인수의 형태를 살펴보면 다음과 같다.

정리 3.7

p가 홀수인 소수이면 M_p의 임의의 소인수 q는 $q \equiv \pm 1 \pmod{8}$의 형태이다.

(증명)

q가 M_p의 임의의 소인수이면 페르마정리에 의해 $2^p \equiv 1 \pmod{q}$이다. 위의 정리 3.6에 의해 q는 임의의 k에 대해 $q=2kp+1$의 형태이므로 $(\frac{2}{q})=1$이면

$$(\frac{2}{q}) \equiv 2^{\frac{q-1}{2}} \equiv 1 \pmod{q}$$

이다.

그러므로 정리 2.11에 의해 $q \equiv \pm 1 \pmod{8}$이 된다. □

2) 메르센느 수와 완전수(Perfect Number)의 관계

고대 그리스 사람들은, 자기 자신의 약수들의 합으로 나타나는 수를 '아르트모스 텔레이오스(Arithmos teleios)'[3]라고 부르며 그들이 알고 있던 네 개의 완전수 6, 28, 496, 8128를 신비한 수로 여겼다. 또한 피타고라스와 그의 제자들은 정수들 중 특별한 의미를 갖는 수에 관심을 갖고 있었으며 '완전수(Perfect Number)'라는 용어를 처음으로 사용하였다. 짝수 완전수와 메르센느 소수는 일련의 관계를 맺고 있다.

정의 3.2

완전수(Perfect Number)란 자신을 제외한 나머지 양의 약수들의 합과 자기 자신이 같은 수를 말한다. 즉, 1보다 큰 정수 n에 대해 양의 약수 전체의 합을 $\sigma(n)$이라고 할 때

$$\sigma(n) = \sum_{d|n} d = 2n$$

이 되는 n을 완전수라고 한다.

양의 정수 중에서 첫 번째 완전수가 되는 6은 양의 약수가 1, 2, 3, 6으로 그 중에서 6을 제외한 약수들의 합이 6=1+2+3이다. 또한 28의 양의 약수들은 1, 2, 4, 7, 14, 28이어서 28=1+2+4+7+14가 되고 496의 양의 약수는 1, 2, 4, 8, 16, 31, 62, 124, 248, 496으로 496=1+2+4+8+16+31+62+124+248이 된다. 실제로 1000이하의 양의 정수들 중에서 완전수가 되는 수는 6, 28, 496뿐이다. 최영한은 53자리 이하의 모든 완전수를 그림으로 소개하였다.[14]

3) 아르트모스 텔레이오스 (Arithmos teleios). 그리스어로 '그 자체로 완성된 수'라는 의미를 지니고 있다.

6
28
496
8,128
33,550,336
8,589,869,056
137,438,691,328
2,305,843,008,139,952,128
2,658,455,991,569,831,744,654,692,615,953,842,176

<그림 1. 53자리 이하의 완전수>

앞에서도 이야기했듯이 고대 그리스인들은 네 개의 완전수를 신비하게 여겨 완전수를 찾는 일을 중요하게 여겼다. 그런데 이러한 완전수의 성질은 메르센느 소수와 밀접한 관련을 맺고 있다. 유클리드는 그의 원론 제 Ⅳ권에서

'2^n-1이 소수이면 $2^{n-1}(2^n-1)$은 완전수이다'

라는 정리를 기재하였으며 또한 그 역이 성립하는 것을 1775년에 오일러가 증명하였다. 즉, 짝수 완전수는 메르센느 소수와 일대일 대응 관계가 되므로 메르센느 소수를 발견하는 것은 짝수 완전수의 발견을 의미하는 것이다.

정리 3.8

n이 양의 정수라고 할 때, $M_n=2^n-1$이 소수이면

$$2^{n-1}M_n=2^{n-1}(2^n-1)$$

은 완전수이다. 역으로 짝수 완전수 n은 적당한 정수 $m\geq 2$에 대해

$$n=2^{m-1}\cdot M_m=2^{m-1}(2^m-1)$$

이다.

(증명)

$M_n=2^n-1$이 소수라 하면 M_n의 양의 약수는 1과 자기 자신 뿐이므로

$$\sigma(M_n) = 1 + M_n = 1 + (2^n - 1) = 2^n$$

이다. 따라서

$$\begin{aligned}\sigma(M_n \cdot 2^{n-1}) &= \sigma(M_n)\sigma(2^{n-1}) \\ &= 2^n \cdot (1 + 2 + 2^2 + \cdots + 2^{n-1}) \\ &= 2^n \cdot \frac{2^n - 1}{2 - 1} \\ &= 2^n(2^n - 1) \\ &= 2 \times 2^{n-1} M_n\end{aligned}$$

이 되어 결국 $2^{n-1}(2^n - 1)$은 완전수이다.

역으로, n이 짝수인 완전수라고 하자. n이 짝수이므로 홀수 k와 $m \geq 2$인 정수 m에 대해

$$n = 2^{m-1}k$$

라 하면 $\gcd(2^{m-1}, k) = 1$이므로

$$\begin{aligned}\sigma(n) &= \sigma(2^{m-1}k) \\ &= \sigma(2^{m-1})\sigma(k) \\ &= \frac{2^m - 1}{2 - 1} \cdot \sigma(k) \\ &= (2^m - 1) \cdot \sigma(k)\end{aligned}$$

이 되고 여기서 n이 완전수가 되기 위해서는 $\sigma(n) = 2n = 2^m k$이어야 하므로

$$\sigma(n) = (2^m - 1) \cdot \sigma(k) = 2^m k$$

이다. 즉, $(2^m - 1) | 2^m k$이다. 그러나 $(2^m - 1, 2^m) = 1$이므로

$$(2^m - 1) | k$$

이 된다. 적당한 정수 $t < k$에 대해 $k = (2^m - 1)t$라 놓고 양의 약수의 합을 구하면

$$\sigma(k) = 2^m t$$

이고 k와 t가 k의 약수이므로

$$\sigma(k) = 2^m t \geq k + t = (2^m - 1)t + t = 2^m t$$

가 되어 결국 k의 양의 약수는 k와 t뿐임을 알 수 있다.

즉, k는 소수이고 $t = 1$이 되어 $k = 2^m - 1$이 된다.

□

위의 정리를 이용하여 6, 28, 496을 메르센느 소수의 곱 형태로 나타내보면 다음과 같다.

$$6 = 1 + 2 + 3 = 2 \cdot 3 = 2^{2-1}(2^2 - 1)$$

$$28 = 1 + 2 + 4 + 7 + 14 = 4 \cdot 7 = 2^{3-1}(2^3 - 1)$$

$$496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248 = 16 \cdot 31 = 2^{5-1}(2^5 - 1)$$

메르센느 수를 이진법으로 나타내면 모든 자리가 1로만 나타난 것과 같이 완전수도 이진법으로 나타내면 일련의 법칙이 존재한다. 메르센느 수 M_n에 대응하는 완전수를 이진법으로 나타내면 자릿수가 $2n-1$자리로 처음 n자리는 1로 나머지 $n-1$자리는 0으로 나타난다. 즉,

$$2^{2-1}(2^2 - 1) = 110_{(2)}$$

$$2^{3-1}(2^3 - 1) = 11100_{(2)}$$

$$\cdots$$

$$2^{n-1}(2^n - 1) = \underbrace{111 \cdots 11}_{n\text{개}}\underbrace{000 \cdots 00}_{(n-1)\text{개}}{}_{(2)}$$

와 같이 나타난다.

정리3.9

n이 짝수 완전수라고 하면, $n \equiv 6 \pmod{10}$ 또는 $n \equiv 8 \pmod{10}$이다.

(증명)

n이 짝수 완전수이므로 위의 정리에 의해 $n=2^{m-1}(2^m-1)$이다. 이 때, 2^m-1이 소수이므로 m도 역시 소수이다.

(ⅰ) $m=2$인 경우

$n=6=2^{2-1}(2^2-1)$이므로 정리가 성립한다.

(ⅱ) $m>2$인 경우

m은 소수이므로 m은 $4k+1$ 또는 $4k+3$의 형태이다.

$m=4k+1$이라 하면

$$\begin{aligned} n &= 2^{4m}(2^{4m+1}-1) \\ &= 2^{8m+1}-2^{4m} \\ &= 2(2^{4m})^2-2^{4m} \\ &= 2\cdot 16^{2m}-16^m \end{aligned}$$

이 된다. 이 때, $16\equiv 6 \pmod{10}$이므로 $16^{2m}\equiv 6^{2m} \pmod{10}$이고 6의 제곱수의 일의 자리 수는 항상 6이므로 $16^{2m}\equiv 6^{2m}\equiv 6 \pmod{10}$이 되어

$$n=2\cdot 16^{2m}-16^{2m}\equiv 2\cdot 6-6=6 \pmod{10}$$

이 된다. 그러므로 $n\equiv 6 \pmod{10}$이다.

$m=4k+3$일 때도 마찬가지로

$$n=2\cdot 16^{2m+1}-2^2\cdot 16^m\equiv 2\cdot 6-2^2\cdot 6=-12\equiv 8 \pmod{10}$$

이 된다. 따라서 $n\equiv 8 \pmod{10}$이다.

□

위의 정리 3.9에 따르면 짝수 완전수는 모두 일의 자리 숫자가 6 또는 8이다. 그러나 6과 8이 교대로 등장하는 것은 아니다. 실제로 <그림 1>을 살펴보면 5번째 완전수은 33,440,336이고 그 뒤에 등장하는 6번째 완전수는 8,589,869,056으로 두

수가 모두 1의 자리 숫자가 6이으로 6과 8이 교대로 등장하지 않는 것을 알 수 있다.

짝수 완전수들의 성질을 더 알아보기 위해 6을 제외한 몇 개의 짝수 완전수들의 각 자리 수들을 더하는 것을 반복하여 한 자리 수가 될 때까지 구해보자. 즉, 28은 각 자리 숫자 2와 8을 더하면 10이 나오고 다시 각 자리 숫자 1, 0을 더하면 1이 된다. 또한 496은 4+9+6=19가 되고 1과 9를 더하면 10이 되므로 다시 1과 0을 더하여 1이 나오고 마찬가지로 8128도 8+1+2+8=19, 1+9=10, 1+0=1이 되어 1임을 알 수 있다. 즉, 6을 제외한 완전수들은 한 자리수가 될 때까지 더하면 1이 된다고 할 수 있다. [12]

정리 3.10

6을 제외한 나머지 짝수 완전수의 각 자릿수들을 더하여, 더한 수가 한 자리수가 될 때까지 계산하면 항상 1이다.

(증명)

$P(x)=\sum_{k=0}^{m} a_m x^k$이라 하자.

어떤 정수 n에 대해 n을 십진법으로 전개하면 적당한 $a_k\,(0 \le a_k < 10)$에 대해

$$n = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$$

이고 n의 각 자리수의 합을

$$S(n) = a_m + a_{m-1} + \cdots + a_1 + a_0$$

이라 하자.

이 때, $n = P(10)$이고 $S(n) = P(1)$임을 알 수 있다. 그런데 $10 \equiv 1 \pmod 9$이므로 $P(10) \equiv P(1) \pmod 9$가 되어 결과적으로 $n \equiv S(n) \pmod 9$이다.

n은 6을 제외한 임의의 짝수 완전수이므로 $n = 2^{m-1}(2^m - 1)$이고 여기에서 $2^m - 1$

은 소수이므로 m도 소수이다. 즉, m이 소수이면 m은 2 또는 3이거나 6으로 나눴을 때 나머지가 1 또는 5이어야 한다.

(ⅰ) $m=2$이면, $n=2^{2-1}(2^2-1)=6$이므로 위 정리에서 제외된다.

(ⅱ) $m=3$이면,

$n=2^{3-1}(2^3-1)=28$이므로 $S(28)=2+8=10$이고 $S(S(28))=1+0=1$이므로

$$28 \equiv S(28) \equiv S(S(28)) \equiv 1 \pmod{9}$$

이다.

(ⅲ) $m=6k+1$일 때, $n=2^{6k}(2^{6k+1}-1)$인데 $2^6 \equiv 1 \pmod{9}$이므로

$$n=2^{6k}(2^{6k+1}-1) \equiv 1(1 \cdot 2-1)=1 \pmod{9}$$

이다.

(ⅳ) $m=6k+5$일 때, $n=2^{6k+4}(2^{6k+5}-1)$이므로 마찬가지로 $2^6 \equiv 1 \pmod{9}$를 이용하면

$$n=2^{6k+4}(2^{6k+5}-1) \equiv 2^4(2^5-1) \equiv 7(5-1) \equiv 1 \pmod{9}$$

이다.

즉, n이 6인 경우를 제외한 짝수 완전수의 자릿수의 합은 항상 $S(n) \equiv 1 \pmod{9}$이다.

□

3. 메르센느 소수 찾기

유클리드가 소수가 무한하다는 것을 증명한 후로 지금까지 큰 소수를 찾는 일은 많은 수학자들의 과제였다. 지금까지 알려진 가장 큰 소수 10개 중 첫 번째부터 9번째 소수까지는 모두 메르센느 소수이며 열 번째 소수는 2007년에 발견된 $19249 \cdot 2^{13018586}+1$으로 그 자릿수가 3,918,990자리이다. 이와 같이 메르센느 소수는 계속해서 가장 큰 소수 기록을 깨고 있다.

2011년 현재까지 발견된 메르센느 소수는 모두 47개이다. 이 중 12개는 전자 컴퓨터가 출현하기 전에 발견된 것이고, 나머지 35개는 전자 컴퓨터의 도움으로 발견된 것이다.

1) 전자 컴퓨터 시대 이전

초기 수학자들은 p가 소수일 때, $M_p = 2^p - 1$과 같은 형태의 수들을 모두 소수라고 여겼다. 그러나 위에서 보인 것과 같이 p가 소수일 때 M_p가 모두 소수인 것은 아니다.

1536년에 레지어스(Hudalricus Regius)는 $p = 11$ 일 때, $M_{11} = 2^{11} - 1 = 2047$이 23과 89의 곱으로 표현될 수 있다는 것을 밝혀내어 가설이 거짓임을 밝혔다. 이 후 1588년 피에트로 카탈디(Pietro cataldi)가 M_{17}과 M_{19}가 소수임을 증명하고, 1603년에 p가 23, 29, 31, 37 일 때도 소수라고 주장하였으나 1640년 페르마(Fermat)를 통해 M_{23}과 M_{37}이 소수가 아님이 밝혀냈다.

이러한 과정을 통해 p가 소수 일 때, $M_p = 2^p - 1$이 소수가 아닐 수도 있다는 것

이 분명해졌으나 p가 어떤 수일 때 M_p가 소수인지 밝히는 데 더 많은 노력이 필요하게 되었다.

1644년 프랑스의 신부 메르센느는 그의 저서인 《물리수학론(Cogitata Physica-Mathematica)》에서

"$n \leq 257$인 $n=2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ 일 때만 2^n-1이 소수이고, 그 외의 나머지 수들에 대해서는 소수가 아니다."

라고 주장하였다. 사실 M_{257}은 그 자릿수가 77자리에 이르는 아주 큰 수이기 때문에 메르센느 자신도 이를 증명하지 못했으나, 당시에 이 주장을 확인할 다른 수학자들도 없었기 때문에 이 주장은 100년가량을 참이라고 인정되었다. 그리고 메르센느의 목록이 완벽하게 고쳐질 때까지는 더 오랜 시간이 소요되었다.

1772년 오일러(Euler)가 M_{31}이 소수임을 증명하였고 1876년에 루카스(Lucas)는 자신이 만든 소수 판정법을 이용하여

$$M_{127} = 170,141,183,460,469,231,731,687,303,715,884,105,727$$

이 소수라고 증명하였다. 이 소수는 전자 컴퓨터 시대가 오기 전까지 손으로 계산한 소수 가운데 가장 큰 소수이다. 또한 1883년 페르부신(Pervouchine)이 M_{61}이 메르센느의 목록에서 빠져 있음을 밝혀내었다.

20세기에 들어선 1903년 10월 뉴욕의 콜럼비아 대학교의 콜(Cole) 교수는 《큰 수의 인수분해》라는 논문을 발표하는 자리에서 M_{67}가 소수가 아님을 증명하였다. 그는 한 마디도 하지 않고 칠판에 나가서

$$2^{67}-1 = 193707721 \times 761838257287$$

라고 썼다. 이를 보고 청중들은 기립 박수를 보냈는데 M_{67}은 1876년에 소수가 아닌 것은 알려졌으나 그 인수분해를 하지 못했었기 때문이다. 그러나 콜 또한 이 인수분해를 3년간 매주 일요일을 바쳐서 계산한 것이었다.

1911년 파워스(Powers)는 《열 번째 완전수》라는 논문을 통해 M_{89}도 소수로 메르

센느의 목록에서 빠져있음을 발표하였고 1914년에 M_{107}이 소수임을 밝혔다.

이러한 수학자들의 적극적인 노력으로 제2차 세계대전이 끝난 후에야 메르센느의 목록이 확정되었는데 이는 다음과 같다.

"$n \leq 257$인 소수 n이 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127 일 때 $2^n - 1$은 소수이고, 나머지는 합성수이다."

2) 전자 컴퓨터시대 이후

전자 컴퓨터의 등장 이후 새로운 컴퓨터의 설계나 설치 시에 그 성능을 시험하기 위해서 큰 소수를 찾거나 소수점 아래의 수십만에서 수십억 자리의 π값을 찾는 방법을 이용하고 있다. 그로 인해 전자 컴퓨터의 등장 이후 엄청나게 큰 메르센느 소수들이 발견되었다.

처음으로 컴퓨터를 이용하여 메르센느 소수를 발견한 사람은 로빈슨(Robinson)으로 1952년 SWAC라는 초기의 컴퓨터를 사용하여 M_{521}, M_{607}, M_{1279}, M_{2203}, M_{2281}이 소수임을 증명하였다. 여기에서 M_{127}과 M_{521}사이에는 더 이상의 소수가 존재하지 않았다. 그 후 베스크(BESK) 컴퓨터로 리젤(Riesel)이 M_{3217}을 발견하였고, 1961년 후르비츠(Hurwitz)가 IBM-7090 컴퓨터를 이용하여 M_{4253}과 M_{4423}을 찾았다.

1963년, 일리노이 대학교 디지털 컴퓨터 연구소의 새 슈퍼컴퓨터 ILLIAC-Ⅱ를 시험하는 과정에서 질리스(Gillies)가 M_{9689}, M_{9941}, M_{11213}을 한꺼번에 발견하였는데 M_{11213}은 그때까지 알려진 가장 큰 소수였던 M_{4423}보다 자릿수가 무려 세 배나 큰 것이었다. 이 발견을 자랑스러워했던 일리노이 대학교 구내 우체국에서는 우편 요금 스탬프에 "$2^{11213} - 1$은 소수다."라는 글을 넣어 이를 기념하였다.

<그림 2. 일리노이 대학교의 우편 요금 스탬프>

8년 뒤에 터커만(Tuckerman)은 IBM360-91을 이용하여 M_{19937}을 발견했다. 1978년 당시에 고등학생이었던 닉켈(Nickel)과 놀(Noll)이 M_{21701}을 발견했다는 사실이 《뉴욕 타임지》의 1면을 장식하였는데, 이는 메르센느 수에 대한 이론을 잘 알지 못했던 두 학생이 이웃에 있는 캘리포니아 헤이워드 주립대학교의 CYBER-174 슈퍼컴퓨터를 440시간이나 실행하여 이뤄낸 쾌거였다. 후에 놀은 M_{23209}를 추가로 발견하였다.

그 후 1996년 위스콘신 주 치피와폴스의 크레이 연구소 공학 및 제조 센터에서 슬로윈스키(Slowinski)가 Cray T94 슈퍼컴퓨터를 이용하여 M_{44497}을 발견한 것을 시작으로 M_{86243}, M_{132049}, M_{216091}, M_{756839}, $M_{1257787}$을 연달아 발견하였다.

같은 해에 아르멩고드(Armengaud)가 개인용 컴퓨터를 이용하여 M_{139269}가 소수임을 밝혔는데 이는 조지 월트만(George Woltman)이 만든 Prime95라는 프로그램 덕분이었다. 이 프로그램은 인터넷 망을 이용, 개인용 컴퓨터에서 소수 검증을 할 수 있게 만든 것으로 월트만은 이 프로그램을 이용하여 GIMPS라는 인터넷 소수 찾기 프로젝트를 만들었다. 이 프로젝트를 통해 35번째 메르센느 소수부터 지금까지 알려진 가장 큰 소수인 $M_{43112609}$까지의 모든 메르센느 소수가 발견되었다. $M_{43112609}$의 자릿수는 12978189이며 이를 text 파일로 저장하면 무려 16.73 MB이며 이를

http://prime.isthe.com/no.index/chongo/merdigit/long-m43112609/prime-c.html

에서 볼 수 있다.

지금까지 발견된 메르센느 소수와 그 발견자에 대한 내용은 다음 장의 표와 같다. 이 표는 The Prime Pages를 참조한 것이다. 이 표에서 연번이 ?인 것은 그 사이에 있는 메르센느 수들의 소수성을 모두 검증하지 못했기 때문이며 그 사이의 메르센느 수가 모두 소수가 아니라는 것이 검증되면 몇 번째 소수라고 정확하게 이름 붙여질 것이다.

연번	p	M_p**의 자릿수**	**발견 연도**	**발견자**	**비고**
1	2	1	미상	미상	
2	3	1	미상	미상	
3	5	2	미상	미상	
4	7	3	미상	미상	
5	13	4	1456	미상	
6	17	6	1588	Cataldi	
7	19	6	1588	Cataldi	
8	31	10	1772	Euler	
9	61	19	1883	Pervushin	
10	89	27	1911	Powers	
11	107	33	1914	Powers	
12	127	39	1876	Lucas	
13	521	157	1952	Robinson	
14	607	183	1952	Robinson	
15	1279	386	1952	Robinson	
16	2203	664	1952	Robinson	
17	2281	687	1952	Robinson	
18	3217	969	1957	Riesel	
19	4253	1281	1961	Hurwitz	
20	4423	1332	1961	Hurwitz	

21	9689	2917	1963	Gillies	
22	9941	2993	1963	Gillies	
23	11213	3376	1963	Gillies	
24	19937	6002	1971	Tuckerman	
25	21701	6533	1978	Noll, Nickel	
26	23209	6987	1979	Noll	
27	44497	13395	1979	Nelson, Slowinski	
28	86243	25962	1982	Slowinski	
29	110503	33265	1988	Colquitt, Welsh	
30	132049	39751	1983	Slowinski	
31	216091	65050	1985	Slowinski	
32	756839	227832	1992	Slowinski, Gage 외	
33	859433	258716	1994	Slowinski, Gage	
34	1257787	378632	1996	Slowinski, Gage	
35	1398269	420921	1996	Armengaud 외	GIMPS
36	2976221	895932	1997	Spence 외	GIMPS
37	3021377	909526	1998	Clarkson 외	GIMPS
38	6972593	2098960	1999	Hajratwala 외	GIMPS
39	13466917	4053946	2001	Cameron 외	GIMPS
?	20996011	6320430	2003	Shafer 외	GIMPS
?	24036583	7235733	2004	Findley 외	GIMPS
?	25964951	7816230	2005	Nowak 외	GIMPS
?	30402457	9152052	2005	Cooper 외	GIMPS
?	32582657	9808358	2006	Cooper 외	GIMPS
?	37156667	11185272	2008	Elvenich 외	GIMPS
?	42643801	12837064	2009	Strindmo 외	GIMPS
?	43112609	12978189	2008	Smith 외	GIMPS

<표 1. 메르센느 소수표>

4. 메르센느 소수 판정

1) 루카스 - 레머 판정법

에두아르 루카스(Edouard Lucas)[4]는 1875년부터 1878년까지 13편의 논문을 통해 메르센느 수가 소수인지 아닌지를 판단하는 소수 판정법을 발표했다. 이는 1장의 페르마의 소 정리인

$$p\text{가 소수이고 } p \nmid a \text{ 이면 } a^{p-1} \equiv 1 \pmod{p}$$

에 근거하는 것이었다. 페르마의 소 정리는 그 역이 성립하지 않는데, 즉, 페르마의 소 정리를 만족하지만 소수가 아닌 수가 존재한다는 것이다. 루카스는 여기에 조건을 추가하여 소수 판정법을 만들었는데 이는 다음과 같다.

'n이 소수인지 여부를 판단한다고 할 때, a가 존재하여 $a^{p-1} \equiv 1 \pmod{n}$이 만족하고 $m=1$부터 $n-1$까지 $a^m \not\equiv 1 \pmod{n}$이면 n은 소수이다.'

이 판정법을 이용하여 루카스는 손으로 계산한 가장 큰 소수인 M_{127}이 소수임을 밝혀내었다. 루카스의 소수 판정법을 이용하면 메르센느의 추측이 틀린 것을 쉽게 알 수 있으나 많은 계산을 필요로 하기 때문에 시간이 오래 걸리는 단점이 있었다. 이러한 단점을 개선하여 1931년 레머(Derrick Henry Lehmer)[5]는 루카스-레머 판정법을 만들었다. 루카스-레머 판정법은 메르센느 소수를 검증하는 가장 획기적이고 편리한 방법으로 GIMPS 프로젝트에서도 이 판정법을 이용하여 메르센느 소수를 검증하고 있다.

---

4) 에두아르 루카스(1842~1891). 파리 천문대에서 르 베리에의 조수로 일하며 수론 및 수론의 역사에 관심을 가지고 수론과, 천문학, 기하학, 해석학, 조합론 등의 분야에 관한 논문뿐 아니라 직조 이론에 관한 논문을 썼다.

5) 데릭 헨리 레머(1905~1991). 수학자였던 부친 데릭 노먼 레머(1867~1938)의 대를 이어 소수연구를 함. 박사학위 논문을 통해 메르센느 소수에 대한 루카스-레머 판정법을 제안하였다.

보조정리 3.11

$S_1 = 4$, $S_{n+1} = S_n^2 - 2$ 인 수열 $\{S_n\}$에 대하여 $w = 2 + \sqrt{3}$ 이고 $v = 2 - \sqrt{3}$ 이라 하면 $S_n = w^{2^{n-1}} + v^{2^{n-1}}$ 이다.

(증명)

귀납법을 이용하여 증명한다.

$n = 1$일 때

$$S_1 = w^{2^0} + v^{2^0} = (2 + \sqrt{3}) + (2 - \sqrt{3}) = 4$$

$n = k$일 때 위의 식이 성립한다고 가정하면 즉,

$$S_k = w^{2^{k-1}} + v^{2^{k-1}} \text{이다.}$$

$n = k+1$일 때

$$\begin{aligned} S_{k+1} &= S_k^2 - 2 \\ &= (w^{2^{k-1}} + v^{2^{k-1}})^2 - 2 \\ &= w^{2^k} + v^{2^k} + 2(wv)^{2^{k-1}} - 2 \\ &= w^{2^k} + v^{2^k} + 2 - 2 \\ &= w^{2^k} + v^{2^k} \end{aligned}$$

이므로 $S_n = w^{2^{n-1}} + v^{2^{n-1}}$이 된다.

□

정리 3.12 루카스-레머(Lucas-Lehmer) 판정법

p가 홀수인 소수일 때, 수열 $\{S_n\}$을 $S_1 = 4$, $S_{n+1} = S_n^2 - 2$이라 하면 $M_p \mid S_{p-1}$ 일 때 그리고 그 때에만 M_p는 소수이다.

(증명)

$M_p | S_{p-1}$이라고 하자.

$w = 2 + \sqrt{3}$, $v = 2 - \sqrt{3}$이라고 하면 보조정리 3.11에 의해 $S_n = w^{2^{n-1}} + v^{2^{n-1}}$이다. $M_p | S_{p-1}$이므로 임의의 정수 R에 대해

$$S_{p-1} = w^{2^{p-2}} + v^{2^{p-2}} = RM_p$$

이다. 위 식의 양변에 $w^{2^{p-2}}$를 곱하면

$$w^{2^{p-2}}(w^{2^{p-2}} + v^{2^{p-2}}) = RM_p w^{2^{p-2}}$$

$$w^{2^{p-1}} + (wv)^{2^{p-2}} = RM_p w^{2^{p-2}}$$

$$w^{2^{p-1}} + 1 = RM_p w^{2^{p-2}}$$

이 되고 1을 이항하면

$$w^{2^{p-1}} = RM_p w^{2^{p-2}} - 1 \quad \cdots\cdots\cdots\cdots\cdots\cdots \quad (1)$$

이 된다. 이를 제곱하면

$$w^{2^p} = (RM_p w^{2^{p-2}} - 1)^2 \quad \cdots\cdots\cdots\cdots\cdots\cdots \quad (2)$$

이다.

이제 M_p가 소수가 아니라고 가정하자. M_p는 합성수이므로 앞의 정리 2.6에 의해 $\sqrt{M_p}$보다 작거나 같은 인수 q가 존재한다.

군 G를 $G = \mathbb{Z}_q[\sqrt{3}]^* = \{a + b\sqrt{3} \mid a, b \in \mathbb{Z}_q\} - \{0\}$이라 하자. 그러면 군 G의 원소의 개수는 $q^2 - 1$개 이고 위의 식 (1), (2)에 의해

$$w^{2^{p-1}} \equiv -1 \pmod{q}$$

$$w^{2^p} \equiv (w^{2^{p-1}})^2 \equiv (-1)^2 \equiv 1 \pmod{q}$$

이다. 따라서 w는 위수 2^p를 가지고 있는 G의 원소이다. 이 때

$$2^p \le q^2 - 1 < M_p = 2^p - 1$$

이므로 모순이 된다.

그러므로 M_p는 소수이다.

그 역의 증명은 생략한다.

□

예를 들어, 루카스-레머 판정법을 이용하여 $M_5 = 2^5 - 1 = 31$ 과 $M_7 = 2^7 - 1 = 127$ 이 소수인지 아닌지를 판정해 보도록 하자. 먼저 $M_5 = 31$이 소수일 필요충분조건은 $M_5 | S_4$이므로 31을 법으로 한 합동식을 계산하면

$$S_1 = 4$$

$$S_2 = 4^2 - 2 = 14$$

$$S_3 = 14^2 - 2 = 194 \equiv 8 \pmod{31}$$

$$S_4 = 8^2 - 2 = 62 \equiv 0 \pmod{31}$$

5는 소수이고 $M_5 | S_4$이므로 결국 $M_5 = 2^5 - 1 = 31$은 소수임을 알 수 있다.

M_7의 경우를 보자. $M_7 = 127$이 소수일 필요충분조건은 $M_7 | S_6$이므로 127을 법으로 한 합동식을 계산하면

$$S_1 = 4$$

$$S_2 = 4^2 - 2 = 14$$

$$S_3 = 14^2 - 2 = 194 \equiv 67 \pmod{127}$$

$$S_4 = 67^2 - 2 = 4487 \equiv 42 \pmod{127}$$

$$S_5 = 42^2 - 2 = 1762 \equiv -16 \pmod{127}$$

$$S_6 = (-16)^2 - 2 = 254 = 127 \cdot 2 \equiv 0 \pmod{127}$$

이 때, $p = 7$은 소수이고 $M_7 | S_6$이므로 따라서 $M_7 = 2^7 - 1 = 127$은 소수라는 결론을 얻는다.

물론 31과 127과 같은 수는 에라토스테네스의 체를 이용하여 $[\sqrt{31}]=5$, $[\sqrt{127}]=11$보다 작은 소수들로 직접 나누어 보는 방법도 가능하다. 그러나

$$M_{127} = 170141183460469231731687303715884105727$$

과 같이 매우 큰 수일 경우에는 루카스 - 레머 판정법을 이용하는 것이 효과적일 것이다.

2) GIMPS와 PrimeNet

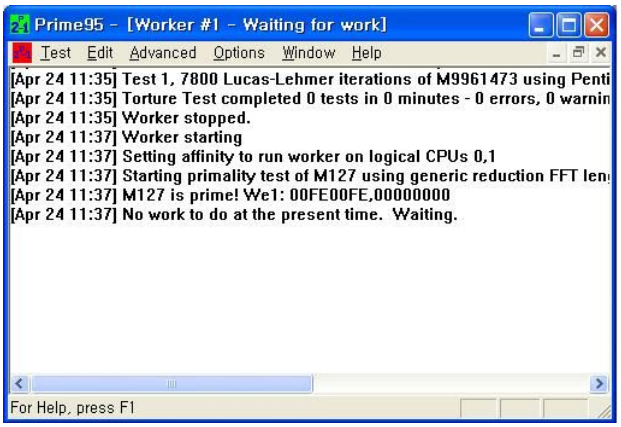
GIMPS는 인터넷을 이용하여 메르센느 소수를 찾는 프로젝트로 'Great Internet Mersenne Prime Search'의 약자이다. 1996년 미국의 프로그래머였던 조지 월트만(George Woltman)은 루카스 - 레머 판정법을 이용하여 소형 컴퓨터에서 쓸 수 있도록 만든 프로그램 Prime95를 개발하여 인터넷에 공개하였는데 이것이 GIMPS의 시작이었다. 그 후 1997년 Scott Kurowski가 PrimeNet이라는 인터넷 서버를 통해 전 세계에 있는 PC사용자들 누구라도 쉽게 이 프로그램을 다운받아 메르센느 소수를 찾을 수 있게 하였다. 현재 GIMPS 홈페이지를 통해 Prime95 프로그램은 26번째 버전이 공개되고 있는데 이를 다운받을 수 있는 GIMPS의 홈페이지 주소는 다음과 같다.

www.mersenne.org

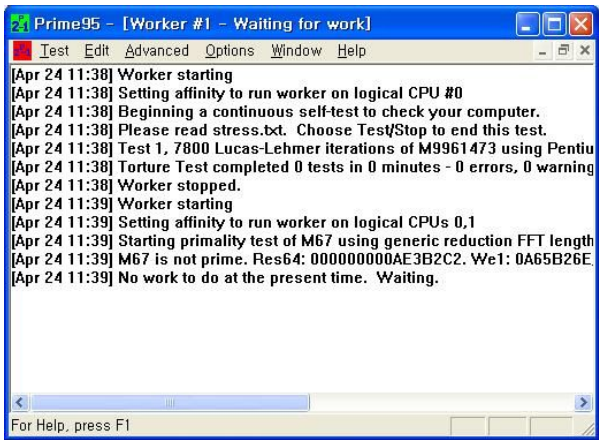
GIMPS 홈페이지를 통해 무료로 다운받아 PC에 설치할 수 있는 이 프로그램은 PC가 인터넷에 연결되어 있는 동안 스스로 할당받은 부분의 계산을 한다. 즉, PrimeNet 서버는 각 사용자들의 PC에 자동으로 지수를 부여하고, 각 PC들은 자동으로 이 지수에 대응하는 메르센느 수에 대해 소수성을 판단하여 다시 메인 서버로 보낸다. 결과적으로 하나의 PC는 거대한 수의 계산에서 아주 작은 역할을 담당

할 뿐이지만 전 세계에서 이 프로젝트에 참여하고 있는 수많은 사용자들의 PC들을 끌어 모으면 엄청나게 큰 병렬처리 기계가 되어 하나의 가상 슈퍼컴퓨터가 되는 것이다. 즉, 이 시스템은 밤낮없이 하루도 쉬지 않고 초당 1조 번의 연산을 실시하는 것이다. 실제로 이를 이용하여 1998년 말까지 백만 자리 이하의 메르센느 수들에 대한 소수성은 모두 조사되었다.

Prime95 프로그램을 통해 M_{127}과 M_{67}의 소수성을 테스트해보도록 하자.



<그림 3. Prime95 - M_{127}>



<그림 4. Prime95 - M_{67}>

이 프로그램을 이용하면 그림 3과 그림 4에서처럼 M_{127}은 소수이고, M_{67}은 소수가 아니라는 것을 짧은 시간 안에 계산하여 알려준다.

GIMPS 프로젝트에는 전 세계에서 20만대 이상의 개인 사용자들이 참여하고 있으며 35번째 메르센느 소수부터는 모두 GIMPS 프로젝트를 통해 발견되고 있다.

많은 사람들이 GIMPS 프로젝트에 참여하는 이유가 좀 더 큰 수 탐색에 대한 지적 호기심 때문만은 아니다. 더 큰 메르센느 소수를 발견하면 큰돈을 벌 수 있는 기회도 주어질 수 있다. 그것은 전자선구자재단(EFF : Electronic Frontier Foundation)[6]에서 수여하는 상금 덕분이다. EFF에서는 1999년 처음으로 백만 자리 이상의 소수 $M_{6972593} = 2^{6972593} - 1$를 발견한 하라트왈라(Hajratwala)에게 5만 달러를 수여하였는데 이는 자릿수가 2098960자리였다. 그 후 천만자리를 넘는 메르센느 소수를 처음으로 발견한 GIMPS에 10만 달러의 상금이 수여되었다. 이에 대한 내용은 GIMPS 홈페이지의 첫 페이지에서 찾아볼 수 있다.

"2009년 10월 14일, GIMPS가 EFF Cooperative Computing Awards에서 상금 10만 달러를 받다! : 당신은 새로운 메르센느 소수를 발견하여 상금을 수상한 다음 사람이 될 수 있는가?

전자선구자재단은 GIMPS에 2008년 8월 23일에 첫 번째 천만 자리 소수에 대한 요구 조건을 모두 충족하는 GIMPS PrimeNet 네트워크에 있는 UCLA 컴퓨터를 통해 45번째로 알려진 12978189 자리의 메르센느 소수 $2^{43112609} - 1$를 발견한 것에 상금 10만 달러를 수여하였다.

… 중략 …

6) 전자선구자재단(EFF : Electronic Frontier Foundation). 1990년 샌프란시스코에 본부를 두고 설립된 비영리 조직. 컴퓨터와 인터넷 영역에서의 표현의 자유와 개인 프라이버시 등 시민들의 권익을 보호하기 위한 목적으로 설립되었다. EFF에서는 'EFF Pioneer Awards'와 'EFF Cooperative Computing Awards'를 통해 인터넷 상에서 지식의 확장을 위해 노력하는 개인이나 조직에 시상하고 있다. 특히, 더 큰 자릿수의 메르센느 소수를 찾으면 'EFF Cooperative Computing Awards'에서 시상과 더불어 상금을 수여하고 있다. 홈페이지 주소는 www.eff.org/awards/coop.html이다.

메르센 소수와 그 역사에 관한 페이지를 봐라. GIMPS는 13년 역사동안 발견된 47개의 메르센 소수 중에 13개를 발견했다."[20]

앞으로 이 재단에서는 1억자리를 넘는 메르센느 소수를 발견하면 15만 달러, 10억자리를 넘으면 25만 달러의 상금을 수여할 예정이다. 이와 같은 행운을 누리기 위해 지금도 많은 사람들이 GIMPS에 참여하고 있다.

5. 메르센느 수와 미해결 문제들.

1) 메르센느의 소수와 합성수는 무한히 많을까?

앞에서 p가 소수일 때, $M_p = 2^p - 1$이 소수일 때를 메르센느 소수라고 하였다. 이 때 메르센느 수 $M_p = 2^p - 1$가 소수가 아닌 수를 메르센느 합성수라고 한다. 이와 같은 메르센느 소수는 각각 짝수 완전수와 일대일 대응이므로 메르센느 소수가 무한할 것인가에 관한 문제는 짝수 완전수는 무한히 많을 것인가와 같은 문제이다. 많은 수학자들이 메르센느 소수가 무한할 것이라고 추측하고 있지만 그 증명이 알려져 있지 않았기 때문에 메르센느 소수가 얼마나 많은지 여부는 알 수가 없다.

리처드는 자신의 저서인 《풀리지 않은 수론 문제(Unsolved Problems in Number Theory)》에서 메르센느 소수에 대해 "그 수효는 의심의 여지없이 무한이지만 그 증명은 절망적일만큼 어렵다."라고 말했다. 그리고 그는 $p \le x$이고 $M_p = 2^p - 1$가 소수인 p의 개수를 의미하는 함수 $M(x)$의 크기에 대한 추정치를 제시하였다. 길리스는 $M(x) \fallingdotseq c\log x$라고 추정하였다. 이 때, c는 e^γ(γ는 오일러 상수)일 가능성이 있다. 또한 포머란스는 $M(x) \fallingdotseq c(\log\log x)^2$라고 추정하였다.

왜그스태프(Wagstaff)의 주장에 의하면 n에 대비하여 $\log p$를 그려 넣는 방식으로 메르센느 소수 $2^p - 1$의 개수를 그래프로 표시하면 곧은 직선을 얻게 되며 이러한 데이터를 바탕으로

1. $M_x \fallingdotseq \dfrac{e^\gamma}{\log 2}(\log\log x)$, $\dfrac{e^\gamma}{\log 2} = 2.5695\cdots$

2. $x < p < 2x$를 만족하는 메르센느 소수 M_p의 개수는 대략 e^γ이다.

3. M_p가 소수일 확률은 대략 $\frac{e^{\gamma}\log ap}{p\log 2}$($a$는 p가 $4n+3$ 형태일 때 2, $4n+1$ 형태일 때 6)이 된다고 한다. 그러나 이 또한 추측에 불과하다.[17]

또한 카탈랑(Catalan)의 추측을 살펴보자. 카탈랑은 다음과 같은 수열에 나타나는 수들은 모두 소수일 것으로 추측하였다.

$$C_1 = 2^2 - 1 = 3$$

$$C_2 = 2^3 - 1 = 7$$

$$C_3 = 2^7 - 1 = 127$$

$$C_4 = 2^{127} - 1 = 170,121,183,460,231,731,687,303,715,884,105,727$$

$$\cdots$$

$$C_n = 2^{C_{n-1}} - 1$$

그러나 C_5는 자릿수가 무려 51,217,599,719,369,681,879,879,723,386,331,576,247자리에 이르는 수로 아직 소수인지 아닌지 판단할 수가 없다. 만약 카탈랑의 추측이 증명가능하다면 메르센느 소수는 무한한 것임이 증명되는 것이지만 아직까지 이는 추측일 뿐이며 많은 수학자들은 이 추측이 맞지 않을 것이라고 예상하고 있다.

메르센느 소수의 무한성 여부와 마찬가지로 메르센느 합성수의 개수 또한 알려지지 않았다. 주어진 메르센느 수가 합성수인지 여부는 그 인수를 통해 알 수 있는데 알려진 메르센느 수중에서 극히 일부만이 인수분해 되어 있다. 그 중에서 50이하의 소수 p에 대해 합성수가 되는 7개의 메르센느 수에 대한 인수분해를 소개하면 다음과 같다.

$$M_{11} = 2047 = 23 \cdot 89$$

$$M_{23} = 8388607 = 47 \cdot 178481$$

$$M_{29} = 233 \cdot 1103 \cdot 2089$$

$$M_{37} = 233 \cdot 616318177$$

$$M_{41} = 13367 \cdot 164511353$$

$$M_{43} = 431 \cdot 9719 \cdot 2099863$$

$$M_{47} = 2351 \cdot 4513 \cdot 13264529$$

오일러는 1750년 만약 $p = 4k+3$이 소수이면 $2^p \equiv 1 \pmod{2p+1}$일 때만 $2p+1$이 소수라는 것을 증명하였다. 이에 따르면 만약 $p = 4k+3$이고 $2p+1$이 소수이면 메르센느 수 $M_p = 2^p - 1$은 합성수가 되는 것이다. 그리고 이를 통해 p, $2p+1$과 같은 무한한 소수의 짝들이 존재한다고 가정할 수 있다. 즉, 이러한 무한한 소수의 짝들이 존재하면 결국 메르센느 합성수가 무한히 많을 수도 있다고 추측할 수 있다. 하지만 아직 이 추측이 사실인지는 알 수 없다.

2) 홀수 완전수는 존재하는가?

앞에서 말한 것과 같이 메르센느 소수와 짝수 완전수는 일대일 대응의 관계를 갖고 있으며 현재까지 알려진 완전수는 모두 짝수이므로 그 개수가 메르센느 소수의 개수와 같다. 이에 과연 홀수 완전수는 존재할 것인지에 대한 의문을 던질 수 있다.

하지스(1973)가 51자리까지의 홀수 중 완전수가 없음을 밝힌 후 블렌트 (Brent, 1991)는 300자리까지 홀수 중에 완전수가 없음을 증명하였다. 그 뒤에 Hagis(1980)와 Sayers(1986), Cohen(1987) 등에 의해 홀수 완전수가 존재한다면 그 수는 완전제곱수와 하나의 홀수인 소수의 제곱수의 곱으로 나타내어질 것이며 그것은 적어

도 8개의 소수로 나눌 수 있고 적어도 29개의 소인수를 가질 것이라는 것을 알게 되었다. 그러나 아직까지 발견된 홀수 완전수는 단 한 개도 없다. 그렇기 때문에 많은 수학자들은 이러한 홀수 완전수의 존재 여부를 회의적으로 생각하고 있다.

컴퓨터가 등장하기 전 수학자들은 오직 자신의 능력만으로 수학 문제를 해결했어야 했는데 사람의 능력은 한계와 시간상의 문제로 인해 오랫동안 해결하지 못한 문제들이 많았다. 그런데 기술의 발달로 인해 컴퓨터를 이용하게 되면서 사람의 능력으로는 해결할 수 없었던 문제들을 해결하는 경우가 종종 있다. 그 중에서도 메르센느 소수는 100여 년 전만해도 100자리 이상의 수도 검증할 수 없을 것이라고 여겨졌으나 100년이 지난 현재 GIMPS를 통해 천만자리 이상의 메르센느 소수가 발견되었고 앞으로 1억자리 이상의 메르센느 소수를 발견하는 것도 머지않아 보인다. 이처럼 기술의 발달을 통해 수학에서 아직 해결되지 않은 문제들을 해결하고 검증하는 등 수학의 발전에 컴퓨터가 크게 기여하고 있다.

이와 같이 메르센느 수에 관한 풀리지 않은 문제들도 컴퓨터 기술의 발전을 통해 문제가 해결되기를 기대해 볼 수 있다. 앞으로 기술이 더욱 발전하여 더 큰 자릿수를 가지는 수들을 검증할 수 있게 되면 아직까지는 단 하나도 발견되지 않았던 홀수 완전수를 발견할 수 있을지도 모른다. 또한 메르센느의 소수와 합성수가 무한한지 여부도 머지않은 미래에 증명될 수 있을 것을 기대해 볼 수 있을 것이다.

참 고 문 헌

[1] 김승욱, 『위대한 수학자들의 사고방식』, 교우사, 2009.

[2] 김응태 · 박승안, 『정수론』, 제 7판, 경문사, 2007.

[3] 허민, 『수학자의 뒷모습 Ⅰ~Ⅳ』, 경문사, 2008.

[4] David M. Burton, 『Elementary Number Theory』, Allyn and Bacon, 1980.

[5] David Wells, 『소수, 수학 최대의 미스터리』, 심재관 옮김, 한승사, 2007.

[6] Keith Devlin, 『수학 : 새로운 황금시대』, 허민 옮김, 경문사, 1999.

[7] Marcus Du Sautoy, 『소수의 음악 : 수학 최고의 신비를 찾아』, 고중숙 옮김, 승산사, 2007.

[8] 민준홍, "메르센 소수에 관하여", 충남대학교 교육대학원 석사학위논문, 2002.

[9] 신근영, "완전수로부터 메르센느 수까지, 그리고 그의 응용", 한남대학교 교육대학원 석사학위논문, 2006.

[10] 안은정, 소수의 특성과 소수 판정에 대한 고찰, 동국대학교 교육대학원 석사학위논문, 2010.

[11] 윤정균, "메르센 소수에 관하여", 충남대학교 교육대학원 석사학위논문, 2000.

[12] 유지선, "메르센 수, 페르마수, 소수 판정법", 수원대학교 교육대학원 석사학위

논문, 2008.

[13] 장창민, “지금까지 알려진 가장 큰 소수”, 인천대학교 교육대학원 석사학위논문, 2007.

[14] 최영한, “이백만 자리를 넘는 소수”, 수학교육논문집 Vol.9, 1999, 165-176p.

[15] J. W. Bruce, “A Really Trivial Proof of the Lucas-Lehmer Test”, The American Mathematical Monthly vol.100 No.4, 1993, 370-371p.

[16] Raphael. M. Robinson, “Mersenne and Fermat Numbers”, Proceedings of the American Mathematical Society vol.5 No.5, 1954, 842-846p.

[17] Samuel S. Wagstaff. Jr, “Divisors of Mersenne Numbers”, Mathematics of Computation vol.40 No.161, 1983, 385-397p.

[18] “1300만 자리 메르센느 소수 발견”, 한국일보, 2008년 9월 29일자, 16면.

[19] 『The Prime Pages』, http://primes.utm.edu/

[20] 『GIMPS』, http://www.mersenne.org/

저작물 이용 허락서

학 과	수학교육	학 번	20088187	과 정	석사
성 명	한글: 김 진 화 한문: 金 珍 華 영문: Kim Jin Hwa				
주 소	광주광역시 광산구 신가동 호반 6차베르디움 606동 602호				
연락처	E-MAIL : jinhwa85@naver.com				
논문제목	한글 : 메르센느 수에 관하여 영어 : A Study of Mersenne Number.				

본인이 저작한 위의 저작물에 대하여 다음과 같은 조건아래 조선대학교가 저작물을 이용할 수 있도록 허락하고 동의합니다.

- 다 음 -

1. 저작물의 DB구축 및 인터넷을 포함한 정보통신망에의 공개를 위한 저작물의 복제, 기억장치에의 저장, 전송 등을 허락함
2. 위의 목적을 위하여 필요한 범위 내에서의 편집·형식상의 변경을 허락함. 다만, 저작물의 내용변경은 금지함.
3. 배포·전송된 저작물의 영리적 목적을 위한 복제, 저장, 전송 등은 금지함.
4. 저작물에 대한 이용기간은 5년으로 하고, 기간종료 3개월 이내에 별도의 의사 표시가 없을 경우에는 저작물의 이용기간을 계속 연장함.
5. 해당 저작물의 저작권을 타인에게 양도하거나 또는 출판을 허락을 하였을 경우에는 1개월 이내에 대학에 이를 통보함.
6. 조선대학교는 저작물의 이용허락 이후 해당 저작물로 인하여 발생하는 타인에 의한 권리 침해에 대하여 일체의 법적 책임을 지지 않음
7. 소속대학의 협정기관에 저작물의 제공 및 인터넷 등 정보통신망을 이용한 저작물의 전송·출력을 허락함.

동의여부 : 동의( ) 반대( )

년 월 일

저작자: 김 진 화 (서명 또는 인)

조선대학교 총장 귀하