韓國數學教育學會誌 시리즈 E
<數學教育 論文集>
제 9집, 1999. 7. 165-176.

J. Korea Soc. Math. Ed. Ser. E:
Communications of Mathematical Education
Vol. 9, July. 1999. 165-176.

이백만 자리를 넘는 소수(素數)[1]

최 영 한 (한국과학기술원)

금년(1999년) 6월 미국 미시간주에 사는 Nayan Hajratwala라는 사람은 2,098,960자리의 소수 $2^{6,972,593}-1$을 발견하였다. 이 소수는 인간이 발견한 소수 중 처음으로 백만자리를 넘는 소수로, 작년에 Clarkson(당시 만 19세)이 발견한 909,526 자리의 소수 $2^{3,021,377}-1$보다 자리수에서 두 배도 더 된다.
현재 백만자리 이하의 모든 메르센 수의 소수성은 검증이 되었다. Spence가 1997년에 발견한 소수 $2^{2,976,221}-1$은 36번째의 메르센 소수로 판명되었고, 작년에 Clarkson이 발견한 소수 $2^{3,021,377}-1$은 37번째의 메르센 소수로 판명되었다. 백만자리까지는 모두 37개의 메르센 소수가 있는 것으로 밝혀졌다. 백만자리를 넘는 메르센 수 중에 이번에 발견한 소수보다 작은 소수가 있는지는 아직 모른다.

1. 천만 자리의 소수에 상금 십만 불

지난 7월 6일자 San Jose Mercury News는 이백만 자리가 넘는 소수(素數) $2^{6,972,593}-1$의 발견을 알렸다. 미국 미시간 주의 작은 도시 Plymouth에 있는 회사 Price Waterhouse Coopers의 기술자문으로 일하는 Nanyan Hajratwala는 자신의 컴퓨터 350 MHz 펜티엄 II의 여유 시간을 111일[2]이나 돌려 십진법으로 2,098,960자리나 되는 큰 소수 $2^{6,972,593}-1$를 발견하였다.

이 소수는 인간이 발견한 소수 중 처음으로 백만 자리를 넘는 소수로, 이제까지 알려진 가장 큰 소수[3]인 $2^{3,021,377}-1$과 비교하여도 자리수에서 두 배도 더 된다.

1cm에 네 자(字)씩 들어가는 크기의 활자를 12포인트라고 하는데 A4 크기의 종이에 2,000 자를 채울 수 있다. 이 크기의 종이 1,050장이 있어야 이번에 발견한 소수를 십진법으로 나타낼 수 있다. 그냥 한 줄로 쓴다면 5.1km나 뻗어 나간다.

현재 천만 자리 소수를 발견하는 사람에게는 Electronic Frontier Foundation[4]에서 상금 십만 불을

---

1) 이 글은 《한국수학교육학회 뉴스레터》 14(3), (1998. 6.) 29~35쪽에 발표한 "가장 큰 소수 찾기"를 근거로 하여 다시 쓴 것이다.

2) 만약 컴퓨터를 쉬지 않고 $2^{6,972,593}-1$ 의 소수성을 조사하였다면 약 20일 걸렸을 것이라고 한다.

3) 1998년 캘리포니아 주립대의 한 시골 캠퍼스 학생 Roland Clarkson(당시 만 19세)이 발견한 909,526 자리의 소수이다.

4) San Francisco에 본부가 있으며 개인 컴퓨터의 여유 시간을 이용하여 컴퓨터 운영 시간이 많이 필요한 일을 돕도록 주선하고 있다. "메르센 소수 찾기"처럼 검증하여야 할 Data가 많고, 또 하나하나의 Data의 검증시간이 많이 필요할 때 이를 여러 컴퓨터에 할당하여 검증하는 일을 돕는다.

내 걸었다.

2. 컴퓨터의 위력

소수의 개념은 간단하지만 아직도 해결되지 않은 문제가 많이 있다. 그래서 소수를 "수론(數論)의 꽃"이라고까지 한다. 소수가 무한히 많이 있다는 증명은 이미 기원전 350년경에 유클리드(Euclid)가 쓴 《원론》(Elements)에 나와 있다.

어마어마하게 큰 소수들은 암호학에서 요긴하게 쓰인다는 것은 잘 알려진 사실이다. 새로운 컴퓨터를 설계하거나 설치하였을 때도 그 성능을 시험하기 위하여 큰 소수를 찾거나 소수점 아래 수십만~수십억 자리의 π값을 찾는다. 최근에는 소수를 찾는 알고리즘을 CPU 성능 검사에 쓰고 있다.

1963년 Gillies, D.B.(1928~75)는 일리노이 대학교 디지털 컴퓨터 연구소의 새 슈퍼컴퓨터 일리악 II의 제어 연결을 시험하는 과정에서 한꺼번에

$$2^{9,689}-1,\ 2^{9,941}-1,\ 2^{11,213}-1$$

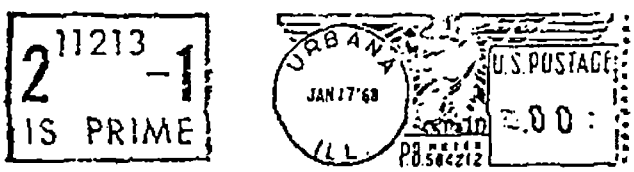
의 세 소수를 발견하였다. 이 소수들은 각각 2,917 자리, 2,993 자리, 3,376 자리의 수였다. 일리악 II의 제어 연결은 Gillies가 고안한 것이었다.

그 때까지 알려진 가장 큰 소수는 바로 2년 전(1961년)에 Hurwitz, A.가 발견한 1,332자리의 소수

$$2^{4,423}-1$$

이였는데 $2^{11,213}-1$은 자리 수에서 세 배나 되었다.

일리노이 대학교 구내 우체국은 우편 요금 스탬프에 "$2^{11213}-1$은 소수"라는 글을 넣어 이 사실을 기념하였고, 이 우체국을 통하여 발송한 우편물에 이 스탬프를 찍어 전세계에 알렸다.



<그림 1> 우편 요금 스탬프

$2^{11,213}-1$도 결국 8년 후 1971년에 Tuckerman이 발견한 6,002 자리의 소수 $2^{19,937}-1$에게 가장 큰 소수의 자리를 내어 주었다.

1978년에는 캘리포니아 주의 남녀 고등학생 Curt Noll과 Laura Nickel이 이웃 대학의 대형 컴퓨터를 440시간이나 돌려 $2^{21,701}-1$를 찾았다.

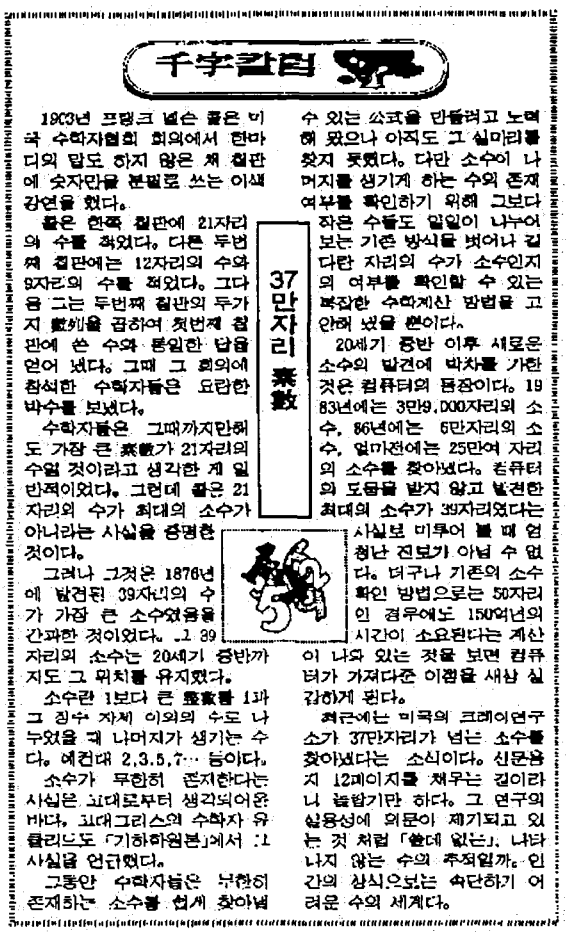
Noll과 Nickel의 "가장 큰 소수 발견"은 New York Times가 1면 기사로 다루었고, 그들의 얼굴은 TV를 통하여 전세계에 방영되었다. 그 후 Nickel은 큰 소수 찾기를 포기하였지만 Noll은 이듬해 (1979년)에 $2^{23,209}-1$을 찾아 또 기록을 세웠다.

이 기록은 오래가지 않았다. 같은 해 Slowinski, D.가 $2^{44,497}-1$을 찾아 기록을 바꾸었다. Slowinski는 1982년, 1983년, 1985년, 1992년, 1994년, 1996년에도 각각

$$2^{86,243}-1,\ 2^{132,049}-1,\ 2^{216,091}-1,\ 2^{756,839}-1,\ 2^{859,433}-1,\ 2^{1,257,787}-1$$

을 발견하여 무려 일곱 번이나 기록을 갱신하였고, "가장 큰 소수 찾기" 최다 기록 보유자가 되었다.

Slowinski가 찾은 $2^{1,257,787}-1$은 37만 자리가 넘는 수로 《한국경제신문》 1996. 9. 6.의 "千字 칼



千字칼럼

37만자리 素數

1903년 프랭크 넬슨 콜은 미국 수학자협회 회의에서 한마디의 말도 하지 않은 채 칠판에 숫자만을 분필로 쓰는 이색 강연을 했다.

콜은 한쪽 칠판에 21자리의 수를 적었다. 다른 두번째 칠판에는 12자리의 수와 9자리의 수를 적었다. 그다음 그는 두번째 칠판의 두가지 數에 곱하여 첫번째 칠판에 쓴 수와 동일한 답을 얻어 냈다. 그때 그 회의에 참석한 수학자들은 요란한 박수를 보냈다.

수학자들은 그때까지만해도 가장 큰 素數가 21자리의 수일 것이라고 생각한 게 일반적이었다. 그런데 콜은 21자리의 수가 최대의 소수가 아니라는 사실을 증명한 것이다.

그러나 그것은 1876년에 발견된 39자리의 수가 가장 큰 소수였음을 간과한 것이었다. 그 39자리의 소수는 20세기 중반까지도 그 위치를 유지했다.

소수란 1보다 큰 整數를 1과 그 정수 자체 이외의 수로 나누었을 때 나머지가 생기는 수다. 예컨대 2,3,5,7… 등이다.

소수가 무한히 존재한다는 사실은 고대로부터 생각되어온 바다. 고대그리스의 수학자 유클리드도 「기하학원론」에서 그 사실을 언급했다.

그동안 수학자들은 무한히 존재하는 소수를 쉽게 찾아낼 수 있는 公式을 만들려고 노력해 왔으나 아직도 그 실마리를 찾지 못했다. 다만 소수이 나머지를 생기게 하는 수의 존재 여부를 확인하기 위해 그보다 작은 수들도 일일이 나누어 보는 기존 방식을 벗어나 길다란 자리의 수가 소수인지의 여부를 확인할 수 있는 복잡한 수학계산 방법을 고안해 냈을 뿐이다.

20세기 중반 이후 새로운 소수의 발견에 박차를 가한 것은 컴퓨터의 등장이다. 1983년에는 3만9,000자리의 소수, 86년에는 6만자리의 소수, 얼마전에는 25만여 자리의 소수를 찾아냈다. 컴퓨터의 도움을 받지 않고 발견한 최대의 소수가 39자리였다는 사실로 미루어 볼 때 엄청난 진보가 아닐 수 없다. 더구나 기존의 소수 확인 방법으로는 50자리인 경우에도 150억년의 시간이 소요된다는 계산이 나와 있는 것을 보면 컴퓨터가 가져다준 이점을 새삼 실감하게 된다.

최근에는 미국의 크레이연구소가 37만자리가 넘는 소수를 찾아냈다는 소식이다. 신문용지 12페이지를 채우는 길이라니 놀랍기만 하다. 그 연구의 실용성에 의문이 제기되고 있는 것 처럼 「쓸데 없는」, 나타나지 않는 수의 추적일까. 인간의 상식으로는 측단하기 어려운 수의 세계다.

<그림 2> 한국경제신문 1996. 9. 6. 38쪽에 난 칼럼

럼"에서도 기사화 되었다. 이 소수도 그해 말에 Armengaud, J.가 찾은 42만 자리가 넘는 소수 $2^{1,398,269}-1$에게 가장 큰 소수의 자리를 내어 주었다.

3. 메르센 소수

이제까지 이야기한 소수들은 모두 2^n-1의 꼴을 갖고 있다. 이런 꼴의 소수를 17세기 프랑스 신부 메르센(Marin Mersenne, 1588~1647)의 이름을 따서 **메르센 소수**라고 한다.

$$3=2^2-1,\ 7=2^3-1,\ 31=2^5-1,\ 127=2^7-1$$

등은 메르센 소수이다. 그러나 2, 5, 11, 13, 17, 19, 23 등은 2^n-1의 꼴로 나타내어지지 않기 때문에 **비**(非) **메르센 소수**라고 한다. 비록 p가 소수일 지라도 2^p-1이 소수가 아닌 수도 있다. 그래서 p가 소수일 때 2^p-1의 꼴의 수를 그냥 **메르센 수**라고 한다.

여기에는 재미있는 역사가 얽혀 있다.

1536년에 Hudalricus Regius가 $2^{11}-1 = 2047$을 23×89로 소인수분해하여 합성수임을 밝히기 전까지 많은 사람들은 p가 소수일 때 메르센 수

$$M_p=2^p-1$$

은 모두 소수라고 생각하였다. M_{13}=8,191은 이미 1456년에 이름을 알 수 없는 사람에 의하여 소수로 밝혀졌다.

1588년에 Pietro Cataldi는 M_{17}과 M_{19}가 소수임을 증명하였다. 그는 또

$$p = 23, 29, 31, 37$$

일 때도 M_p는 소수라고 하였는데, M_{31}만 소수이고 나머지는 모두 합성수이다.[5]

1644년 메르센은 그의 저서 《물리·수학론》(Cogitata Physica-Mathematica)의 머리말에서

$$p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$$

일 때 M_p는 모두 소수라고 하였다. 그러나 M_{67}과 M_{257}은 합성수임이 각각 259년과 287년이 지난

5) 1640년에 페르마(Pierre de Fermat, 1601~1665)는 M_{23}과 M_{37}이 합성수임을 보였다. M_{29}가 합성수인 것은 메르센이 보인 듯하다. 과학자들은 17세기를 "아마추어 수학자 시대"라고 하는데 페르마, 메르센 등 취미로 수학을 연구하는 사람이 많았기 때문이다. M_{31}은 1772년에 오일러(Leonhard Euler, 1707~1783)가 소수임을 증명하였다.

후(1903년과 1931년)에 밝혀졌다. 그는 또 $p \leq 257$ 인 지수 중에서 메르센 소수를 만드는 지수인 61, 89, 107을 빠트렸다.[6]

1876년 Lucas는 메르센 수의 소수성을 알아내는 Lucas 판정법을 만들고, 이 판정법을 이용하여 M_{127}이 소수임을 증명하였다.

Lucas가 1876년 소수라고 밝힌 39자리의 수

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

은 1952년까지 무려 76년 동안이나 "알려진 가장 큰 소수"의 자리를 지켰다. M_{127}은 컴퓨터를 쓰지 않고 찾은 가장 큰 소수이다.[7]

1883년에 Pervushin은 메르센이 빠트린 M_{61}을 찾았고, Powers, R.E.도 메르센이 빠트린 또 다른 두 소수 M_{89}와 M_{107}을 각각 1911년과 1914년에 찾았다.

---

6) 메르센이 제시한 지수에서 실제로 소수를 만드는 지수는 Cataldi가 제시한 지수들 보다 겨우 하나(p=127)가 더 많다.

컴퓨터가 어느 정도 발달한 후인 1947년에야 비로소 $p \leq 257$ 인 지수 범위내에서는

$$p = 2,3,5,7,13,17,19,31,61,89,107,127$$

밖에는 메르센 소수를 만드는 지수가 더 없음을 증명하였다. $M_p = 2^p - 1$ 이 소수가 되는 지수 p에 대해서는 Cataldi가 먼저 제시하였으나 후세 사람들은 $2^p - 1$인 꼴의 소수를 "메르센 소수"라고 한다. 이는 아마도 그의 저서 《물리·수학론》 때문인 것 같다.

7) Leonard E. Dickson이 쓴 "수론의 역사"(History of the Theory of Numbers, 1919년에 Carnegie Institute of Washington에서 발행, 1971년에 Chelsea에서 영인본 발행)의 제1권 22쪽에 Lucas가 1876년 M_{127}이 소수라고 밝힌 직후 Eugene Charles Catalan(1814-1894)은

$$\begin{aligned}
C_1 &= 2^2 - 1 = 3 \\
C_2 &= 2^3 - 1 = 7 \\
C_3 &= 2^7 - 1 = 127 \\
C_4 &= 2^{127} - 1 = 170,141,183,460,469,231,731,687,303,715,884,105,727 \\
C_5 &= 2^{170,141,183,460,469,231,731,687,303,715,884,105,727} - 1 = ? \\
&\cdot \\
&\cdot \\
&\cdot
\end{aligned}$$

로 이어지는 수열에 나타나는 수는 모두 소수일 것이라고 예상하였다. 그러나

$$C_5 = 2^{170,141,183,460,469,231,731,687,303,715,884,105,727} - 1$$

은 십진법으로 나타냈을 때 벌써 그 자리 수에서 51,217,599,719,369,681,879,879,723,386,331,576,247자리나 되는 큰 수이다. 아직 아무도 C_5의 소수성에 도전할 엄두를 못 내고 있다.

만약 이 수열에 나타나는 수가 모두 소수라면 메르센 소수는 무한히 많이 있는 것이 되어 또 하나의 미해결 문제가 해결되는 셈이다. 그러나 많은 소수 연구가들은 Catalan의 예상(Conjecture)을 부정적으로 보고 있다. 그 이유는 $M_{13} = 8191$은 소수이지만 $M_{8191} = 2^{8191} - 1$ 은 합성수이기 때문이다.

1903년에 Cole, F.N.은 미국수학회의 모임에서 M_{67}을 193,707,721×761,838,257,287로 소인수분해 됨을 보였는데 Eric Temple Bell(1883~1960)이 쓴 《수학, 과학의 여왕이면서 하인》(Mathematics, Queen and Servant of Science; 1951)에 마침 그 장면이 들어 있어 번역하지 않고 그대로 옮겨보겠다.

> At the October, 1903, meeting in New York of the American Mathematical Society, Frank Nelson Cole, a Columbia University professor, had a paper on the program with modest title on the factorization of large numbers.
>
> When the chairman called on him for his paper, Cole—who was always a man of very few words—walked to the board and, saying nothing, proceeded to chalk up the arithmetic for raising 2 to the sixty-seventh power. Then he carefully substracted 1. Without a word he moved over to a clear space on the board and multiplied out, by longhand,
>
> 193,707,721×761,838,257,287.
>
> The two calculations agreed. Mersenne's conjecture—if such it was—vanished into the limbo of mathematical mythology. For the first and only time on record, an audience of the American Mathematical Society vigorously applauded the author of a paper delivered before it. Cole tooked his seat without having uttered a word. Nobody asked him a question.
>
> Years later, when I asked Cole in 1911 how long it had taken to crack M_{67}, he said "three years of Sunday."

1931년에 Lehmer, D.H.(1905~)는 Lucas 판정법을 고쳐 Lucas-Lehmer 판정법을 만들었다.

Lucas-Lehmer 판정법

$\{S_n\}$을 $S_1=4$, $S_{n+1}=S_n^2-2$로 정의된 수열이라 하자.
p가 홀수이면 메르센 수 $M_p=2^p-1$은 M_p가 S_{p-1}을 나눌 때 또 그 때만 소수이다.

Lehmer는 이를 이용하여 메르센이 소수라고 한 마지막 M_{257}도 합성수임을 보였다.

컴퓨터를 써서 메르센 소수를 찾는 데 처음으로 성공한 사람은 Robinson, R.M.이다. 그는 1952년에 무려 다섯 개의 메르센 소수

$$M_{521},\ M_{607},\ M_{1,279},\ M_{2,203},\ M_{3,217}$$

을 찾았다. 1876년에 Lucas가 찾은 M_{127}은 39 자리의 수인데 반해 Robinson이 찾은 소수들은 각각 157 자리, 183 자리, 386 자리, 664 자리, 687 자리로 자릿수에서 모두 네 배 이상 뛰었다. 그리고 M_{127}과 M_{521}사이에는 더 이상 메르센 소수가 없었다.

4. GIMPS와 PrimeNet

최근에 알려진 가장 큰 소수의 기록을 세운 소수들은 모두 메르센 소수이다. 그 이유는 메르센 수의 소수성에 대해서는 Lucas-Lehmer 판정법이라는 비교적 쉬운 판정법과 GIMPS라는 프로그램 때문이다. GIMPS는 1996년에 George Woltman이 만든 프로그램 Great Internet Mersenne Prime Search의 약자이다.

Woltman은 Lucas-Lehmer 판정법을 소형 컴퓨터(PC, Mac, Unix)에도 쓸 수 있도록 프로그램을 개발하여

http://www.mersenne.org/prime.htm

에 올려 놓았다. 이 프로그램으로 찾은 메르센 소수들이 최근에 찾은 5개의 소수이다.

CPU 생산업체로 잘 알려진 인텔(Intel)은 펜티엄 칩을 출하하기 전에 월트만 프로그램으로 성능을 검사하고 있다.

Scott Kurowski는 1997년에 PrimeNet이라는 Internet Server를 만들어 전세계 월트만 프로그램 사용자들이 서로 협력하여 새로운 메르센 소수를 찾도록 하였다.[8)]

PrimeNet가입자들은 1998년 말까지 백만 자리보다 작은 메르센 수들의 소수성은 모두 조사하였다. 그리하여 Spence가 1997년에 발견한 소수 $M_{2,976,221}$이 36번째의 메르센 소수임을 알았고, Clarkson이 1998년 초에 발견한 소수 $M_{3,021,377}$도 37번째의 메르센 소수임을 알았다. 그러나 아직 백만 자리를 넘는 메르센 수들 중에서 이번에 발견한 소수 $M_{6,972,593}$보다 작은 소수가 있는지는 모른다.

5. 홀수인 완전수는 있는가?

6의 약수 중 6보다 작은 수 1, 2, 3을 모두 합치면 6이 된다. 또 28의 약수 중 28보다 작은 수 1, 2, 4, 7, 14를 모두 합치면 28이 된다. 이 같이 어떤 수에서 자신보다 작은 약수를 모두 합치면 원래의 수가 될 때 이 수를 **완전수**(perfect number)라 한다.

기원전 그리스 시대에 이미 네 개의 완전수 6, 28, 496, 8128을 알고 있었지만 완전수는 그리 흔하

8) 현재 전세계 약 12,600명의 PrimeNet 가입자들이 있다. 이들에 의하여 연결된 컴퓨터만도 21,500대이며 이 컴퓨터들은 지수를 나누어 여유 시간에 메르센 수의 소수성에 대해서 조사하고 있다. Internet PrimeNet Server는 각 가입자들의 컴퓨터에 자동적으로 지수를 부여하고, 각 컴퓨터는 여유 시간에 자동적으로 이 지수에 대응하는 메르센 수의 소수성에 대하여 조사한다. 또 조사가 끝났을 때는 본부의 컴퓨터에 이 사실이 입력되고 대형 컴퓨터로 한 번 더 소수성에 대하여 검증을 한다.
PrimeNet 가입자들 중에는 초·중·고등학교 교사들도 많이 있는 데 그들은 학생들이 수학에 흥미를 느끼게 하는데 이 Internet Server을 이용하고 있다.

지 않다. 아래 수들은 53자리 이하의 완전수를 모두 나타낸 것이다.

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 3> 53자리 이하의 완전수

2^p-1 이 소수이면 $2^{p-1}(2^p-1)$ 은 완전수인 것은 이미 유클리드의 《원론》에 증명이 있다. 그런데 18세기 중엽에 오일러가 모든 짝수인 완전수는 $2^{p-1}(2^p-1)$ 의 꼴로 나타내어지며 이 때 2^p-1 은 소수인 것을 증명하였다. 따라서 짝수인 완전수의 개수와 메르센 소수의 개수는 같다.

완전수와 관련하여 아직도 해결되지 않은 문제가 많이 있다. 그 중에서도 다음 두 문제는 소수 연구가들에게 오래 동안의 관심사였다.

첫째, 과연 홀수인 완전수는 존재하는가?
둘째, 메르센 소수는 무한히 많이 있는가?

우선 첫째 문제 해결의 진척 사항을 알아보자. Hagis(1973)는 먼저 51자리까지의 홀수 중에는 완전수가 없음을 밝혔다. 또 Brent et al(1991)은 300자리까지의 홀수 중에는 완전수가 없음을 밝혔다.

Hagis(1980)에 다시 홀수인 완전수가 존재한다면 그 수는

$$p_1^{a(1)}\ p_2^{a(2)}\ \cdots\ p_t^{a(t)} \tag{1}$$

($t \geq 8$, $p_1, p_2, \cdots, p_t$는 모두 홀수인 서로 다른 소수, $p_1 \equiv a(1) \equiv 1 \pmod 4$, $i=2,3,\cdots,t$일 때 $a(i)$는 짝수)로 소인수분해 되어야 한다는 것을 알았다.

또 Sayers(1986)는 (1)에서 $a(1)+a(2)+\cdots+a(t) \geq 29$를 찾아내었고, 다시 Cohen(1987)은

p_1, p_2, …, p_t 중 적어도 한 소수는 21자리보다 큰 것을 밝혔다. 그러나 아직도 홀수인 완전수는 찾지 못하였다.

따라서 이제까지 발견한 메르센 소수의 개수와 완전수의 개수는 같다.

<표 1>는 $M_p=2^p-1$ 이 메르센 소수이고, $P_p=2^{p-1}(2^p-1)$ 이 완전수가 되는 지수 p 중에서 지금까지 찾은 것을 모두 열거한 것이다.

<표 1> 메르센 소수와 완전수

순서	지수 p	M_p의 자릿수	P_p의 자릿수	발견연도	발견자
1	2	1	1	—	—
2	3	1	2	—	—
3	5	2	3	—	—
4	7	3	4	—	—
5	13	4	8	1456	—
6	17	6	10	1588	Cataldi
7	19	6	12	1588	〃
8	31	10	19	1772	Euler
9	61	19	37	1883	Pervushin
10	89	27	54	1911	Powers
11	107	33	65	1914	〃
12	127	39	77	1876	Lucas
13	521	157	314	1952	Robinson
14	607	183	366	1952	〃
15	1279	386	770	1952	〃
16	2203	664	1327	1952	〃
17	2281	687	1373	1952	〃
18	3217	969	1937	1957	Riesel
19	4253	1281	2561	1961	Hurwitz
20	4423	1332	2663	1961	〃
21	9689	2917	5834	1963	Gillies
22	9941	2993	5985	1963	〃
23	11213	3376	6751	1963	〃
24	19937	6002	12003	1971	Tuckerman
25	21701	6533	13066	1978	Noll & Nickel
26	23209	6987	13973	1979	Noll
27	44497	13395	26790	1979	Nelson & Slowinski
28	86243	25962	51924	1982	Slowinski
29	110503	33265	66530	1988	Colquitt & Welsh
30	132049	39751	79502	1983	Slowinski
31	216091	65050	130100	1985	〃
32	756839	227832	455663	1992	Slowinski & Gage
33	859433	258716	517430	1994	〃
34	1257787	378632	757263	1996	〃
35	1398269	420921	841842	1996	Armengaud, et. al.
36	2976221	895932	1791864	1997	Spence, et. al.
37	3021377	909526	1819050	1998	Clarkson, et. al.
?	6972593	2098960	4197919	1999	Hajratwala, et. al.

6. 숫자 1로만 된 소수

메르센 소수를 컴퓨터가 좋아하는 이유 중 하나는 이들을 이진법으로 나타내었을 때 모든 자리에 숫자 1이 나타나기 때문이다.[9]

이제 메르센 소수의 이야기는 이 정도로 하고 다른 모양의 소수에 관하여 이야기하여 보자.

십진법으로 나타내었을 때 모든 자리에 한가지 숫자로만 된 수를 repunit 수라고 하는데 여기서는 1이 n번 나타나는 수

$$R_n=(10^n-1)/9$$

만 관심이 있다. 2, 3, …, 9 중 한 숫자가 모든 자리에 나타나는 수는 소수가 아니기 때문이다.

영국의 퍼즐 전문가 Dudeney, H.E.는 그의 저서 《캔터버리의 수수께끼》 (The Canterbury Puzzles; 1907)에 $R_2=11$ 은 숫자 1만으로 된 유일한 소수라 하고, R_3, R_4, …, R_{18}이 모두 합성수임을 보였다. 그런데 이 책을 읽은 한 독자 Oscar Hope이 19자리의 수

$$1{,}111{,}111{,}111{,}111{,}111{,}111$$

이 소수임을 밝혔다. 그는 계속하여 R_{23}도 소수임을 밝혔다.

여기서도 R_n이 소수이기 위해서는 n이 소수이어야 한다. 그러나 p가 소수라고 하여 반드시 R_p가 소수가 되는 것은 아니다.

R_{29}, R_{31}, R_{37}, R_{41}, R_{43}, R_{53}, R_{61}, R_{73}가 합성수라는 것은 진작 알려졌으나 R_{47}, R_{71}이 합성수인 것을 밝힌 것은 그렇게 오래되지 않는다. 그 이유는 이들이 굉장히 큰 소인수를 갖고 있기 때문이다. $R_{71}=(10^{71}-1)/9$ 는 1984년에 Los Alamos연구소에서 슈퍼컴퓨터 Cray를 써서

$$241{,}573{,}142{,}393{,}627{,}673{,}576{,}957{,}439{,}049$$
$$\times 45{,}994{,}811{,}347{,}886{,}846{,}310{,}221{,}728{,}895{,}223{,}034{,}301{,}839$$

로 30자리의 소수와 41자리의 소수의 곱으로 소인수분해 하였다(Williams, 1984).

Williams & Dubner(1986)는 그들이 개발한 알고리즘으로 10,000 보다 작은 소수 p에 대하여 R_p가 소수인 것을 모두 찾았는데

---

9) 메르센 수 $M_p = 2^p-1$은 이진법으로 나타냈을 때 p자리의 수가 되는데 모든 자리에 1이 된다. 또 메르센 소수 M_p에 대응하는 완전수 $P_p = 2^{p-1}(2^p-1)$은 처음 p자리에 1만 나타나고, 다음 p-1 자리에는 0만 나타난다. 따라서 2^p-1이 소수일 때 $2^{p-1}(2^p-1)$이 완전수인 것은 쉽게 증명할 수 있다.

$$R_2,\ R_{19},\ R_{23},\ R_{317},\ R_{1031}$$

외에는 repunit 소수가 없었다. 10,000 자리보다 큰 repunit 소수는 아직 찾지 못하고 있다.

7. 가장 큰 쌍둥이 소수

11과 13, 17과 19, 29와 31 등과 같이 두 수의 차이가 2인 두 소수를 "쌍둥이 소수"라고 한다. 현재 알려진 가장 큰 쌍둥이 소수는 Indlekofer, K.H.와 Járai, A.가 1996년에 발견한

$$697053813\times 2^{16352}-1,\ 697053813\times 2^{16352}+1$$

이다. 그런데 1997년에 Forbes, T.는 486컴퓨터로

$$6797727\times 2^{15328}-1,\ 6797727\times 2^{15328}+1$$

과 같은 상당히 큰 쌍둥이 소수를 발견하였다. 쌍둥이 소수가 무한히 많이 있는지도 현재 밝혀지지 않은 문제이다.

참 고 문 헌

김응태 · 박승안 (1997). 정수론 제4판, 서울: 경문사, pp.39-74.

이명옥 · 김은주 · 박정숙 (1998). 소수(Prime Number) 이야기, 수학사랑 **11**, pp.2-7.

최영한 (1966). 소수에 관한 문제, 한국수학교육학회지 시리즈 A 《수학교육》 **4(2)**, pp.43-51.

최영한 (1998). 가장 큰 소수 찾기, 한국수학교육학회 뉴스레터 **14(3)**, pp.29-35.

Brent, R.P.; Cohen, G.L. & te Riele, H.J.J. (1991). Improved Techniques for Lower Bounds for Odd Perfect Numbers, *Math. Comp.* **59**, pp.857-868.

Devlin, K. (1997). World's Largest Prime, *Focus(News. Math. Assoc. Amer.)* **17(6)**, p.1.

Gillies, D.B. (1964). Three New Mersenne Primes and a Statistical Theory, *Math. Comp.* **18**, pp.93-97.

Hagis, P. (1973). A Lower Bound for the Set of Odd Perfect Numbers, *Math. Comp.* **27(124)**, pp.951-953.

Hagis, P. (1980). Outline of a Proof that Every Odd Perfect Number has at Least Eight Prime Factors, *Math. Comp.* **35(151)**, pp.1027-1032.

Ribenboim, P. (1995a). Selling Primes, *Math. Mag.* **68(3)**, pp.175-182.

Ribenboim, P. (1995b). *The New Book of Prime Number Records, 3rd Ed.*, New York: Springer-

Verlag.

Williams, H.C. (1984). Factoring on a Computer, *Math. Intelligencer* **6(3)**, pp.29-36.

Williams, H.C. & Dubner, H. (1986). The Primality of R_{1031}, *Math. Comp* **47(176)**, pp.703-711.