뤼카-레머 소수 판별법

Student ID: 20170616

Name: 정희진

1. 서론

오늘날 사람들은 큰 소수를 찾기 위해 노력하고 있다. 큰 소수를 찾으면 수업시간에 배웠던 것처럼 암호학에서 큰 역할을 할 수 있다. 어떤 수가 소수인지를 결정하는 방법은 여러가지가 있지만 그 숫자가 커질수록 소수인지 판별하기 위한 계산은 훨씬 많아지고 이를 계산하기 위한 시간도 많아진다. 따라서 시간복잡도가 보다 낮은 알고리즘을 찾아야 한다. 이 보고서에는 어떤 메르센 수가 소수인지를 판별할 수 있는 뤼카-레머 소수 판별법에 대해 소개를 할 것이다. 현대에 알려진 큰 소수는 메르센 소수인 경우가 많다.

2. 메르센 소수란 무엇인가

메르센 수는 2의 거듭제곱에서 1이 모자란 수를 가리킨다.

$$\mathrm{M_n} = 2^{\mathrm{n}} - 1 \ \ (\mathrm{n}\text{은 } 0 \text{ 또는 자연수})$$

다음 수들은 메르센 수를 나타낸다.

0, 1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, 8191, 16383, 32767, 65535, 131071, 262143, 524287, 1048575, 2097151, 4194303, 8388607, 16777215, 33554431, 67108863, 134217727, 268435455, 536870911, 1073741823, 2147483647, 4294967295

여기서 메르센 소수란 메르센 수이면서 소수인 수를 말한다. 다음은 메르센 소수를 나타낸다.

3, 7, 31, 127, 8191, 131071, 524287, 2147483647, 2305843009213693951, 618970019642690137449562111, 162259276829213363391578010288127, 170141183460469231731687303715884105727

메르센 수에 관한 여러가지 이론들이 있는데, 그중 하나는 다음과 같다.

메르센 수($\mathrm{M_n} = 2^{\mathrm{n}} - 1$)가 소수면 n은 소수다.

증명을 하면 다음과 같다.

n이 0, 1일때는 메르센 수가 각각 0, 1이다.

$\mathrm{n} \geq 2$일 때는 먼저 n이 합성수라고 가정한다. 그렇다면 $\mathrm{n} = \mathrm{ab}$ $(\mathrm{a}, \mathrm{b}$는 1보다 큰 자연수$)$로 나타낼 수 있다. 그러면

$$\mathrm{M_n} = 2^{\mathrm{n}} - 1 = 2^{\mathrm{ab}} - 1 = \ (2^{\mathrm{a}} - 1)((2^{\mathrm{a}})^{\mathrm{b}-1} + (2^{\mathrm{a}})^{\mathrm{b}-2} + \cdots + 2^{\mathrm{a}} + 1)$$

따라서 메르센 수 M_n은 합성수가 된다. 어떤 명제가 참이면 그 대우 또한 참이므

로 메르센 수($M_n = 2^n - 1$)가 소수면 n은 소수이다.

3. 뤼카-레머 소수 판별법이란 무엇인가

뤼카-레머 소수 판별법은 어떤 메르센 수가 소수인지를 알 수 있게 해준다. 이는 메르센 수($M_n = 2^n - 1$)에서 n이 홀수인 소수일 때만 적용가능하다. 참고로 위에서 메르센 수가 소수면 n은 소수라고 증명하였다. 따라서 n이 0, 1일때는 메르센 수가 각각 0, 1로 소수가 아니고, n이 합성수 일 때는 메르센 수가 합성수가 된다. 또한 n이 2(짝수인 소수)일 때는 메르센 수는 $M_n = 2^2 - 1 = 3$이 되므로 소수라는 것을 알 수 있다. 따라서 위와 같은 사실과 더불어 뤼카-레머 소수 판별법을 이용하면 n의 값에 상관 없이 임의의 메르센 수가 소수인지 아닌지를 판별할 수 있게 된다.

이제 뤼카-레머 판별법에 대해 알아보자. 어떤 메르센 수 ($M_n = 2^n - 1$, n은 홀수인 소수)가 있다고 생각하자. 그리고 수열 S_i를 다음과 같이 정의하자.

$$S_i = \begin{cases} 4 \ \ (i = 0\text{일 때}) \\ S_{i-1}^2 - 2 \ \ (i > 0\text{일 때}) \end{cases}$$

다음 수들은 수열 S_i를 나타낸 것이다.

4, 14, 194, 37634, 1416317954, 2005956546822746114, 4023861667741036022825635656102100994, 1619146272111567178177755907012051366495859012549915851432930874097 5788034

"$S_{n-2} \equiv 0 \pmod{M_n}$" 와 "$M_n$는 소수"는 동치이다. 따라서 어떤 메르센 수가 소수인지 판별하기 위해 $S_{n-2} \equiv 0 \pmod{M_n}$인지를 확인하면 된다.

위와 같은 판별법이 왜 맞는지 증명을 해보자($S_{n-2} \equiv 0 \pmod{M_n}$이면 M_n는 소수임을 증명).

$\omega = 2 + \sqrt{3}, \overline{\omega} = 2 - \sqrt{3}$라고 하자. 그렇다면 다음과 같은 이유로 $S_i = \omega^{2^i} + \overline{\omega}^{2^i}$이다.

$$S_0 = \omega^{2^0} + \overline{\omega}^{2^0} = \left(2 + \sqrt{3}\right) + \left(2 - \sqrt{3}\right) = 4$$

$i = n - 1$일 때 $S_i = \omega^{2^i} + \overline{\omega}^{2^i}$이 성립한다고 가정하자.

$$\begin{aligned} S_n &= S_{n-1}^2 - 2 \\ &= \left(\omega^{2^{n-1}} + \overline{\omega}^{2^{n-1}}\right)^2 - 2 \\ &= \omega^{2^n} + \overline{\omega}^{2^n} + 2(\omega\overline{\omega})^{2^{n-1}} - 2 \\ &= \omega^{2^n} + \overline{\omega}^{2^n} \end{aligned}$$

$i=n$일 때 $S_i=\omega^{2^i}+\overline{\omega}^{2^i}$이 성립하므로 모든 i에 대해 $S_i=\omega^{2^i}+\overline{\omega}^{2^i}$이다.
$S_{n-2}\equiv 0 \pmod{M_n}$이라고 가정하자. 그렇다면,

$$\omega^{2^{n-2}}+\overline{\omega}^{2^{n-2}}=kM_n \ (k\text{는 정수})$$
$$\omega^{2^{n-2}}=kM_n-\overline{\omega}^{2^{n-2}}$$
$$(\omega^{2^{n-2}})^2=kM_n\omega^{2^{n-2}}-(\omega\overline{\omega})^{2^{n-2}}$$
$$\omega^{2^{n-1}}=kM_n\omega^{2^{n-2}}-1$$

M_n가 합성수라하고 q를 M_n의 가장 작은 소수인 인수라고 하자. M_n은 홀수이므로 $q>2$이다. Z_q를 modulo q의 정수 집합, $X=\{a+b\sqrt{3}|a,b\in Z_q\}$라고 하자. $q>2$이므로 $\omega\in X$이다. 다음으로 X안에서의 곱셈을 다음과 같이 정의하자.

$$(a+\sqrt{3}b)(c+\sqrt{3}d)=[(ac+3bd)\mathrm{mod}\ q]+\sqrt{3}[(ad+bc)\mathrm{mod}\ q]$$

따라서 X의 원소와 X의 원소를 위의 곱셈에 따라 곱하면 그 결과도 X의 원소가 된다. X^*는 X의 원소들의 역수들로 이루어진 집합이라고 하자. X의 원소인 0은 역수가 없으므로 $|X^*|\le|X|-1=q^2-1$이다. $M_n\equiv 0 \pmod q, \omega\in X$이므로

$$kM_n\omega^{2^{n-2}}=0 \ \text{in}\ X$$
$$\omega^{2^{n-1}}=-1 \ \text{in}\ X$$
$$\omega^{2^n}=1 \ \text{in}\ X$$
$$\omega\omega^{2^{n-1}}=1 \ \text{in}\ X$$

따라서 ω는 $\omega^{2^{n-1}}$의 역수이고 $\omega\in X^*$이다. $\omega^{2^n}=1$ in X이고 $\omega^{2^{n-1}}=-1$ in X이므로 ω의 차수는 2^n이다. 원소의 차수는 집합의 차수보다 같거나 작으므로

$$2^n\le|X^*|\le q^2-1<q^2$$

q는 M_n의 가장 작은 소수인 인수이므로

$$q^2\le M_n=2^n-1$$

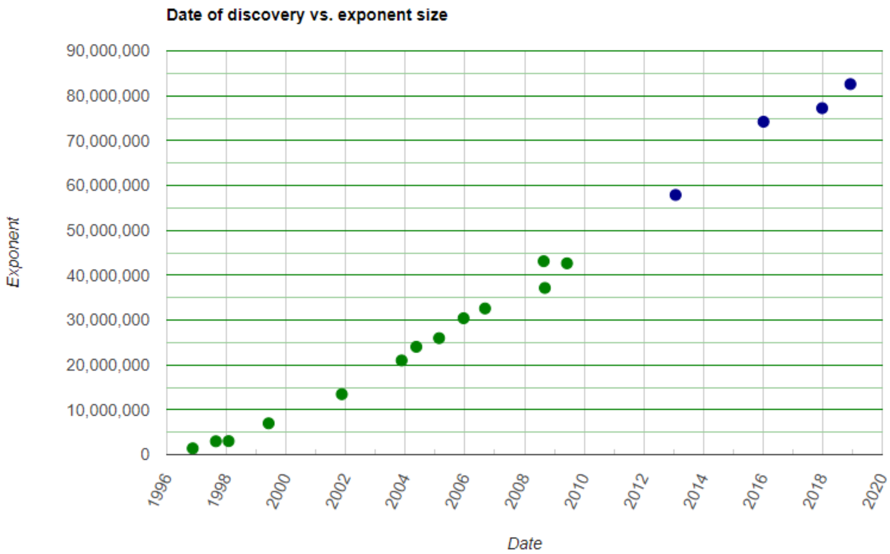
$2^n<2^n-1$은 모순이므로 M_n은 소수이다.
역으로 M_n이 소수면 $S_{n-2}\equiv 0 \pmod{M_n}$임을 증명할 수 있는 방법도 있지만 위 증명만으로도 $S_{n-2}\equiv 0 \pmod{M_n}$을 이용해 소수임을 판별할 수 있으므로 증명을 나타내지 않았다.
 뤼카-레머 소수 판별법의 시간 복잡도는 $O(n^3)$이다. 하지만 n-bit의 두 수를 곱하기 위해서 Schönhage–Strassen algorithm이나 Fürer's algorithm을 사용하면 시간복잡도를 더 줄일 수 있을 것이다.

4) GIMPS란 무엇인가

 GIMPS란 Great Internet Mersenne Prime Search의 소프트웨어를 이용해 메르센 소수를 찾은 프로젝트이다. 현재까지 발견된 메르센 소수는 다음과 같다.

#	2^p-1	Digits	Date Discovered	Discovered By
1	$2^{2}-1$	1	c. 500 BCE	Ancient Greek mathematicians
2	$2^{3}-1$	1	c. 500 BCE	Ancient Greek mathematicians
3	$2^{5}-1$	2	c. 275 BCE	Ancient Greek mathematicians
4	$2^{7}-1$	3	c. 275 BCE	Ancient Greek mathematicians
5	$2^{13}-1$	4	1456	Anonymous
6	$2^{17}-1$	6	1588	Pietro Cataldi
7	$2^{19}-1$	6	1588	Pietro Cataldi
8	$2^{31}-1$	10	1772	Leonhard Euler
9	$2^{61}-1$	19	1883	Ivan Mikheevich Pervushin
10	$2^{89}-1$	27	1911 Jun	R. E. Powers
11	$2^{107}-1$	33	1914 Jun 11	R. E. Powers
12	$2^{127}-1$	39	1876 Jan 10	Édouard Lucas
13	$2^{521}-1$	157	1952 Jan 30	Raphael M. Robinson
14	$2^{607}-1$	183	1952 Jan 30	Raphael M. Robinson
15	$2^{1,279}-1$	386	1952 Jun 25	Raphael M. Robinson
16	$2^{2,203}-1$	664	1952 Oct 07	Raphael M. Robinson
17	$2^{2,281}-1$	687	1952 Oct 09	Raphael M. Robinson
18	$2^{3,217}-1$	969	1957 Sep 08	Hans Riesel
19	$2^{4,253}-1$	1,281	1961 Nov 03	Alexander Hurwitz
20	$2^{4,423}-1$	1,332	1961 Nov 03	Alexander Hurwitz
21	$2^{9,689}-1$	2,917	1963 May 11	Donald B. Gillies
22	$2^{9,941}-1$	2,993	1963 May 16	Donald B. Gillies
23	$2^{11,213}-1$	3,376	1963 Jun 02	Donald B. Gillies
24	$2^{19,937}-1$	6,002	1971 Mar 04	Bryant Tuckerman
25	$2^{21,701}-1$	6,533	1978 Oct 30	Landon Curt Noll & Laura Nickel
26	$2^{23,209}-1$	6,987	1979 Feb 09	Landon Curt Noll
27	$2^{44,497}-1$	13,395	1979 Apr 08	Harry Lewis Nelson & David Slowinski
28	$2^{86,243}-1$	25,962	1982 Sep 25	David Slowinski
29	$2^{110,503}-1$	33,265	1988 Jan 28	Walter Colquitt & Luke Welsh
30	$2^{132,049}-1$	39,751	1983 Sep 19	David Slowinski
31	$2^{216,091}-1$	65,050	1985 Sep 01	David Slowinski
32	$2^{756,839}-1$	227,832	1992 Feb 19	David Slowinski & Paul Gage
33	$2^{859,433}-1$	258,716	1994 Jan 04	David Slowinski & Paul Gage
34	$2^{1,257,787}-1$	378,632	1996 Sep 03	David Slowinski & Paul Gage
35	$2^{1,398,269}-1$	420,921	1996 Nov 13	GIMPS / Joel Armengaud
36	$2^{2,976,221}-1$	895,932	1997 Aug 24	GIMPS / Gordon Spence
37	$2^{3,021,377}-1$	909,526	1998 Jan 27	GIMPS / Roland Clarkson
38	$2^{6,972,593}-1$	2,098,960	1999 Jun 01	GIMPS / Nayan Hajratwala
39	$2^{13,466,917}-1$	4,053,946	2001 Nov 14	GIMPS / Michael Cameron
40	$2^{20,996,011}-1$	6,320,430	2003 Nov 17	GIMPS / Michael Shafer
41	$2^{24,036,583}-1$	7,235,733	2004 May 15	GIMPS / Josh Findley
42	$2^{25,964,951}-1$	7,816,230	2005 Feb 18	GIMPS / Martin Nowak
43	$2^{30,402,457}-1$	9,152,052	2005 Dec 15	GIMPS / Curtis Cooper & Steven Boone
44	$2^{32,582,657}-1$	9,808,358	2006 Sep 04	GIMPS / Curtis Cooper & Steven Boone
45	$2^{37,156,667}-1$	11,185,272	2008 Sep 06	GIMPS / Hans-Michael Elvenich
46	$2^{42,643,801}-1$	12,837,064	2009 Jun 04	GIMPS / Odd M. Strindmo
47	$2^{43,112,609}-1$	12,978,189	2008 Aug 23	GIMPS / Edson Smith
48*	$2^{57,885,161}-1$	17,425,170	2013 Jan 25	GIMPS / Curtis Cooper
49*	$2^{74,207,281}-1$	22,338,618	2016 Jan 07	GIMPS / Curtis Cooper
50*	$2^{77,232,917}-1$	23,249,425	2017 Dec 26	GIMPS / Jon Pace
51*	$2^{82,589,933}-1$	24,862,048	2018 Dec 07	GIMPS / Patrick Laroche

다음 그래프는 각 연도마다 찾은 메르센 소수를 나타낸다(세로축은 $M_n = 2^n - 1$에서 n을 나타낸다). 그래프가 일차함수와 가까운 형태로 나타나므로 각 연도마다 몇 자리의 메르센 소수가 발견될지 예측할 수 있다.



참고문헌

1) https://en.wikipedia.org/wiki/Lucas%E2%80%93Lehmer_primality_test

2) https://oeis.org/A003010

3) https://en.wikipedia.org/wiki/Mersenne_prime

4) https://oeis.org/A000225

5) https://oeis.org/A000668

6) https://en.wikipedia.org/wiki/Order_(group_theory)

7) https://ko.wikipedia.org/wiki/GIMPS

8) https://www.mersenne.org/primes/