韓國數學敎育學會誌〈數學敎育〉
1977. 6, Vol. XV No. 2

Journal of the Korea Society of Mathematical Education
Jun. 1977. Vol. XV No. 2

素數를 구하는 다른 한 가지 방법

淸州大學 李 康 燮

〔註〕 다음 글은 Mathematics Teacher Vol. 69 No. 5 pp. 398~400, 1976. 5. 에 실린 D. B. Cohen의 글을 번역한 것이다.

역사적으로, 여흥적이고 실제적인 흥미때문에 수학자들은 完全數와 Mersenne 素數를 연구하여 왔다. 本 考의 목적은 Mersenne 數가 素數인지 合成數인지를 판단하는 기준을 논의하는데 있다.

完全數는 어떤 數의, 자신을 제외한 約數의 총합이 그 數와 같아지는 것을 말한다. 예를 들어서 6은 6을 제외한 약수 1, 2, 3의 합이 6이므로 完全數이다. 같은 방법으로 28=1+2+4+7+14 이므로 28은 完全數이다. 6과 28은 (古來로부터) 完全하다고 생각되어져왔고, 우주의 창조가 6일에 이루어졌고 달의 주기가 28일 이라는 것으로 부터 (完全하다는 것이) 실증되었다.

2,000여년 전 Euclid는 p와 2^p-1이 素數일 때 $2^{p-1}(2^p-1)$의 형태의 모든 수는 짝수인 完全數임을 증명하였다. 예를 들어서 $p=2$라 하면 2^p-1은 $2^2-1=3$이므로 $p=2$는 完全數를 구하는 공식에 사용될 수 있다. $p=2$를 대입하면 최초의 完全數 $2^{2-1}(2^2-1)=2\times3=6$을 얻는다. 18세기에 Euler는 Euclid의 공식이 모든 짝수인 完全數에 적용됨을 증명하였다. Euclid의 공식에 의하여 주어지는 처음부터 5번째 까지의 完全數는 6, 28, 496, 8128, 3350336이다.

Euclid의 공식에 의하면, 素數 p를 2^p-1이 素數가 되도록 놓는 것만이 허용된다. $M_p=2^p-1$이라하자. 따라서 $M_3=2^3-1=7$, $M_5=2^5-1=31$ 등등이다. 만약 M_p가 素數이면, 특별히 이 M_p를 Mersenne 素數라 한다. 이 이름은 17세기의 수학자 Marin Mersenne에서 따온 것이다. 예를 들어, $M_3=2^3-1=7$은 素數이므로 7은 Mersenne 素數이다. 현재까지 Mersenne 素數가 되는 素數 p는 다음과 같은 24개만 알려졌다.

2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937.

이것은 素數들 가운데 Mersenne 素數가 되지 않은 것을 뺀 것으로 이해된다. 예를 들어 $p=11$에 대하여 $M_{11}=2^{11}-1=2047=89\times23$ (이므로 위의 24개의 수 가운데 들어가지 못한다.) 덧붙여 만약 n이 合成數이면 M_n은 合成數임이 명백하다. 실제로, $2^{ab}-1=(2^a-1)\{(2^a)^{b-1}+\cdots\cdots+1\}$ $(a>1,\ b>1)$이므로 2^a-1 나누어 떨어진다. 또한 각별히, n이 2보다 큰 짝수이면 M_n은 合成數이다.

1772년 Euler는 $M_{31}=2147483647$이 素數임을 밝혔고 이 수는 100년 이상이나 가장 큰 素數로 알려져왔다. E. V. Lucas는 어떤 주어진 素數 p에 대하여 M_p가 素數인지 아닌지를 판단하는 멋진 檢證을 개발하였다. 그 결

과는 나중에 D. H. Lehmer에 의하여 수정되었고 증명이 간단히 되었다. Lucas-Lehmer 수열이라고 불리는 다음 數들의 수열을 생각해 보자,

4, 14, 194, 37634, 1416317954, ……

이 수열은 점화식

$S_1=4,\ S_{k+1}=S_k^2-2,\ k=1,2,3,\cdots\cdots$

을 만족한다. 즉 $14=4^2-2,\ 194=14^2-2\cdots$

아래 定理는 1930년 발표된 Lehmer의 논문에서 증명되었다.

〔定理〕 M_n이 素數일 必要充分條件은 S_{n-1}이 M_n으로 나누어질 때이다.

예를 들어, M_5가 素數인지 아닌지를 알려고 한다고 하자. 첫째로 $M_5=2^5-1=31$을 계산한다. 다음, S_4가 31로 나누어지는가를 검토한다. 만약 나누어지면 M_5는 素數이고 나누어지지 않는다면 合成數이다. $37634=31\times 1214$이므로 $M_5=31$은 素數이다. 이것은 우리가 알고있는 31에 대하여 쉽게 (素數라는 것이) 검토 된다. 만약 M_{29}가 素數인지를 판단하기를 원한다면 위 수열의 28항 (S_{28})이 M_{29}로 나누어 떨어지는 가를 검토하면 된다. Lucas-Lehmer 검증 방법은 長點과 短點을 모두 갖고 있다. 長點은 이 방법이, Mersenne 數가 素數인가를 검토하는데 있어서(전통적인 방법으로) 그들의 제곱근보다 작은 素數들로 나누어볼 필요성이 없다는데 있다. 短點은 이 數例 (4, 14, 194, …)이 매우 급속히 증가하는데 있다. (각 항의 자릿수가 전항의 자릿수의 거의 2배가 된다.) 이러한 短點때문에, 동시에 M_n에서 자릿수를 2번 이상 처리하지 못한다. 만약 어떤 검증하고자 하는 수가 있다면 M_n을 法으로 하여, 項들을 되풀이하여 감소시키면서 數列을 만든다. 예를 들어 M_7이 素數인가를 검증하고자 한다고 하자. 우리는 $M_7=2^7-1=127$ 보다 큰 數를 얻을 때 까지 (S_k의) 數列 4, 14, 194를 만들어야 한다. 194를 127로 나누어서 나머지 67을 얻는다. 194를 67로 대치한 다음 수열 4, 14, 67, 4487를 얻는다. (여기서 4487은 67^2-2에서 계산된다. $S_{k+1}=S_k^2-2$ 참조) 4487을 127로 나누어서 나머지 42를 얻는다. 4487을 42로 대치한 다음 수열 4, 14, 67, 42, 1762를 얻는다. 이러한 방법을 계속하여 數列 4, 14, 67, 42, 111, 0을 얻는다. 6번째 項 0은 127로 나누어지므로 $M_7(=127)$은 素數이다. M_n을 法으로 하여 감소시키는 것에 대한 타당성은, 감소된 數列과 원래의 數列이 一般的으로, $a\equiv b \pmod t$이면 $a^2-2\equiv b^2-2 \pmod t$이기 때문에 M_n을 法으로 하여 合同이다. 이런 방법으로 數列의 126번째 항의 계산에 의하여 Lucas는 M_{127}(39자릿수)가 素數임을 증명하였다. 이것은 탁상계산기가 Computer로 대치되는 1950년대까지 가장 큰 素數로 남아 있었다.

마지막 예로 $M_6=2^6-1$이 素數인가를 판단하려고 한다고 하자. Lucas 數列 $S_1=4,\ S_{k+1}=S_k^2-2$ 즉 4, 14, 194, …를 M_6을 法으로 하여 변형하면 4, 14, 5, 23, 23이다. 이 數列의 제5항이 63을 法으로하여 0이 아니기 때문에 63은 素數가 아니다.

Lucas 검증에 대한 가장 간단한 FORTRAN 프로그램은 다음과 같다.

```
      DOUBLE PRECISION X, Y, DMOD
      DO 50 J=3, 27
      Y=2. DO**J-1. DO
      X=4. DO
      JO=J-2
      DO 80 I=1, JO
      X=X**2-2
      X=DMOD(X, Y)
   80 PRINT53, X
   53 FORMAT('', D23. 16)
      IF(X. EQ. 0)GO TO 20
      PRINT 11, Y
   11 FORMAT('', F16. 0,' IS COMPOSITE')
      GO TO 50
   20 PRINT 10, Y
   10 FORMAT('', F16. 0, 3X,' IS PRIME')
```

```
50  PRINT 90
90  FORMAT('',1X)
    STOP
    END
```

Mn(n=3, 4, ⋯, 27)을 검증하는 프로그램은 double precision을 사용한다. 이 프로그램을 약간 수정함으로써 M_n을 n이 56일때도 검증할 수 있다. 함수 DMOD는 어떤 數 X를 가지며, 그것은 Y를 法으로 하여 환산된다. 끝으로, 홀수 n에 대하여 Mn을 검증하기를 원한다면($n>2$인 짝수이면 앞에서 본 바와 같이 Mn은 합성수이다) 프로그램의 두번째 명제를 DO 50 J=3, 27, 2로 수정하여야 한다. 고등학교 학생들은 아마 현재 사용하는 BASIC 대신에 手動전자계산기나 위에 기술된 것과 유사한 새로운 컴퓨터프로그램을 사용함으로써 Lucas 검증을 도구로 할 수 있다.

Beiler는 1964년 Lucas검증의 사용의 흥미있는 역사적인 설명을 주었다. 1936년 I. Krieger는 5년간의 노력끝에 M_{257}이 素數임을 증명했었다고 보고 하였다. M. Kraitchik는 1922년에, O. H. Lehmer는 1931년에 Lucas 검증을 사용하여 M_{257}이 합성수임을 증명하였다. Lehmer의 작업은 탁상계산기를 이용하여 700시간이 걸렸다. 이 문제는 1953년 SWAC(Standard Western Automatic Computer)에 의하여 48초 만에 M_{257}이 合成數임이 결정되었다. Lucas검증이, 어떤 數가 素數인가 아닌가를 결정하는 것은 흥미있지만 그것의 약수들은 알 수가 없다. 즉, 우리는 78자릿수 M_{257}이 合成數임은 알지만 아직 M_{257}의 약수는 아직 아무것도 알지 못한다.

1974년 까지 24개의 Mersenne 素數(따라서 24개의 짝수인 完全數)가 발견되었다. 제 24번째 Mersenne 素數 M_{19937}은 6002 자릿수인데 이것은 1971년 3월 New York에 있는 IBM Thomas Watson 연구센터에서 발견되었다. 이것이 아직까지 알려진 가장 큰 素數이다. 이 數에 관련된 完全數는 $2^{19936}(2^{19937}-1)$로서 12003 자릿수이다.

參 考 文 獻

Beiler, Albert H. Recreations in the Theory of Numbers—The Queen of Mathematics Entertains. New York: Dover Publications, 1964.

Kraitchik, M. Théorie des Nombres. Vol. 2. Paris: Gauthier-Villars, 1922.

Lehmer, D. H. "Note on Mersenne Numbers." Bulletin of the American Mathematical Society 38 (1932):383.

—— "On Lucas' Functions." Annals of Mathematics 31(1930):419—48.

Lucas, E. V. "Théorie des Fonctions Numériques Simplement Periodiques." American Journal of Mathematics 1 (1877):184—239, 289—321.