素數에 關한 問題

崔 英 瀚

Y. H. Choe: *Topics in Prime Number Theory.*

目 次

0. 序 論

19 世紀의 大數學者 Gauss 는 "整數論은 數學의 女王"이라고 하였고, "*The Queen of the Science*" (科學의 女王, 1931)의 著者 Eric Temple Bell 은 "數學은 科學의 女王"이라고 하였다. 그러면 여기에서 整數論의 王座에는 누구를 앉히느냐가 문제가 된다. 두 말할 것도 없이 "素數의 理論"이 그 王座를 차지할 것이다.

現在의 많은 教科書들이 素數에 關하여 紙面을 割愛하고 있다. 그 具體的인 理由는 여러가지 있겠지만 대개 다음의 두가지 理由를 들 수 있겠다.

첫째, 이 분야가 數學的인 심오한 理論을 必要로 하지 않으면서 젊은 사람들에게 어렵고 未解決된 問題를 提示하여 줄 수 있다는 것이다. 다시 말하면 비록 學生들이 數學에 關한 知識이 充分하지 않더라도 재미나는 數學問題를 다룰 수 있다는 것이다. 素數에 關한 몇몇 理論은 問題가 提示된 後 2000 年 동안 아무도 解決하지 못하였지만, 또 어떤 問題는 쉽게 學生들이 理解할 수 있는 것이 있다.

두째, 整數論의 여러 分野中에서 素數의 研究보다 더욱 興味있고 神秘스러운 分野는 없을 것이다. "1 과 自己自身외에는 나누어 지지 않는 수" 이렇게 定義하면 1 도 素數에 包含하게 되므로 "1 외에"라는 말을 더 붙인다. ("自然數중에서 約數가 둘 뿐인 數"로 定義하는 경우도 있다.) 素數에 關係되는 여러 問題중 몇가지는 너무나 쉬어서 國民學校 學生들도 理解할 수 있지만, 대부분은 아직 大數學者도 아마 "解가 없을 것이다."라고 할 정도로 問題를 解決하기는 아직 너무나 막연하다. 素數問題가 어렇게 취급되는 理由는 여러가지 있겠지만 그중 重要한 原因은 "素數는 아직 確實한 묘사(?)를 할려는 모든 企圖를 거부하지만, 그러나 確實히 랜덤(무작의)하지는 않게 흩어져 있다"는 것 때문일 것이다.

무릇 數學의 歷史上에서 素數의 問題만큼 論難의 對象이 되고 問題의 未解決이 오래 계속된 것도 없다. 우리는 지금 素數의 어떤 性質을 알고 있으며 또한 어떠한 問題가 未解決인지 알고 싶다. 또 그 未解決은 어느 程度 진척되고 있는가 궁금한 경우가 많다. 여기에 對하여 近刊 外國의 會誌를 通하여 본 것을 몇가지 추려보고

끝으로 素數의 "領域" (Domain) (素數를 定義하는 領域)을 바꾸면 어떤 結果가 나타나는가를 살펴보기로 하자.

1. n 번째 素數는 무엇인가?

이에 對答하는 단 한가지 方法으로 우리들은 素數의 數列을 가져와서 n 번째까지 세는 수 밖에 없다.

그러면 이 素數의 數列은 어떻게 얻는가?

여기에서 가장 간단한 方法은 自然數의 數列에서 "合成數" (素數가 아닌 數)를 모두 除去하는 것이다. 물론 이러한 作業을 電子計算機는 굉장한 速力으로 해 나간다. 그러나 아직은 지금으로부터 2000년전에 아르키메데스(Archimedes)의 친구인 에라토스테네스(Erathosthenes)가 考案한 方法을 쓰고 있다. [1] 그러면 그가 考案한 "체"(Sieve) (이것을 "에라토스테네스의 체"라고 한다.)에 의하여 1에서 100까지의 素數를 골라내는 方法을 研究하여 보자.

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50	51	52	53	54
55	56	57	58	59	60
61	62	63	64	65	66
67	68	69	70	71	72
73	74	75	76	77	78
79	80	81	82	83	84
85	86	87	88	89	90
91	92	93	94	95	96
97	98	99	100		

그림 1 에라토스테에스의 체

우선 오른편 그림과 같이 1에서100까지를 여섯줄로쓴다. 다음두째줄, 네째줄, 여섯째줄을 수직으로 내려 그어서 2만 제외하고 2의 배수를 모두 除去한다. 다음은 3을 제외하고 세째줄을 아래로 내려 그어므로서 3의 배수를 모두 除去한다. 다음은 5을 제외하고 왼쪽으로 대각선으로 내려 그어므로서 5의 배수를 除去한다. 다음은 7를 除外하고 오른쪽으로 對角線으로 내려 그으므로서 7의 倍數를 모두 除去한다. 다음은 11의 倍數가 되겠지만 11은 이 그림에서 제일 큰 수인 100의 제곱근 보다 크므로 100이하의 素數는 모두 찾아 낸 셈이다. (여기에 관하여는 다시 뒤에 설명하겠다.) 만약에 100이상 더 많은 수가 있다면 좀 더 가파른 對角線으로 11의 倍數를 모두 除去하고, 다음은 13의 倍數를 모두 제거하고, 이렇게 자꾸 合成數를 제거하므로서 結局 素數만 남게된다. 이 作業을 電子計算機는 기억장치에 依하여 광장히 빠른 速力으로 해 나간다. 美國의 Los Almos 과학연구소의 電子計算機는 9천만 개의 素數를 기억하고 있다고 한다. 그러면 다시 1에서 100까지의 自然數로 돌아가서 아직 체에 남아 있는 數는 26개이다. 이중 1을 제외하고 25개의 素數를 얻는다.

2. 쌍둥이 素數

또 앞서 예를 든 1에서 100까지의 에라토스테네스의 체를 보면 3보다 큰 모든 素數는 6의 倍數보다 1이 작던지 1이 큰 것을 알 수 있다. 이와같이 素數에서는 "쌍둥이 素數" (두 素數의 차가 2인 素數)가 많다는 것을 알 수 있다. 즉 71과 73, 209,267과 209,269 또는 1,000,000,009,649와 1,090,000,009,651등이 되겠다. 그러면 이와 같은 數는 어떻게 하여 生成되는가 보자.

우선 自然數에서 2 또는 3의 倍數를 모두 제거하므로서 남는 것은 모두 "쌍둥이 數"(素數이던 아니던 간에)이다. 그러나 계속하여 체질하므로서 이들 쌍둥이 數의 한쪽 또는 양쪽을 제거하게 되지만 아직 많은 數가 그대로 남게 된다. 그러나 이 쌍둥이 素數도 數가 커짐에 따라 귀하게 된다. 그렇지만 쌍둥이 素數가 無限히 계속되리라고 가정하고 있다. 그러나 아직 아무도 확실한 근거는 찾지 못하였다.

3. 素數의 密度

앞서 에라토스테네스는 自然數를 6列의 直四角形으로 配列하였지만 이것을 다른 方法으로 配列한다면 素數의 分布는 어떤 모양으로 나타

날 것인가? [2]

지금 오른편 그림과 같이 중앙에 1을 쓰고 시계방향의 나선(螺旋)으로 四角形의 格子속에 自然數를 써 나간다면 소수의 배열은 다른 모양으로 나타날 것이다.

이것을 보면 螺旋의 가운데 부분에서는 素數들이 열을 지어 있게 되는 데, 이것은 이부분의 密度가 크고, 또 2를 제외한 모든 素數는 홀수이기 때문이라고 생각되기 때문에 수가 더욱 크지고 소수의 밀도가 희박한 곳에서도 이러한 열을 이룰 것이라는 것을 기대하기는 어렵다. 그러면 이것을 더 많은 數로 확장하면 어떤 모양이 될가?

100	99	98	**97**	96	95	94	93	92	91
65	64	63	62	**61**	60	**59**	58	57	90
66	**37**	36	35	34	33	32	**31**	56	**89**
67	38	**17**	16	15	14	**13**	30	55	88
68	39	18	**5**	4	**3**	12	**29**	54	87
69	40	**19**	6	1	**2**	**11**	28	**53**	86
70	**41**	20	**7**	8	9	10	27	52	85
71	42	21	22	**23**	24	25	26	51	84
72	**43**	44	45	46	**47**	48	49	50	**83**
73	74	75	76	77	78	**79**	80	81	82

그림 2

아래의 왼편 그림은 이것을 1에서 10,000까지 확장한 것이고, 오른편 그림은 1에서 65,000까지 확장한 것이다. 그러나 여기서 우리는 두 그림의 가장자리 부분에서도 素數들이 列을 이루고 있는 것을 알 수 있다. 그러면 이러한 열을 식으로 나타낼 수 없을가? 또 어떠한 열이 가장 많은 비율의 素數를 包含하고 있을가? 하는 생각이 든다.

그래서 우리가 처음 시도한 것이 x^2+x+5이다. 그러나 이것은 x가 0에서 3까지일 때는 素數이지만 4일 때는 5의 倍數가 된다는 것을 알 수 있다. 그리하여 다음으로 시도한 것이 18世紀의 大數學者 오일러가 생각하였던 식 x^2+x+17이다.

오일러(Leonhard Euler)는 1707年 스위스의 바아젤에서 태어나서 1725年 러시아 女皇帝 애카테리나 1세에 초대되어 페테스부르그大學(지금의 레닌그라드에 있었음)의 교수가 되었으나 불행히도 1735年 오른쪽 눈을 잃고, 1771年 왼쪽 눈을 마저 잃어 장님이 되었으나 13년동안을

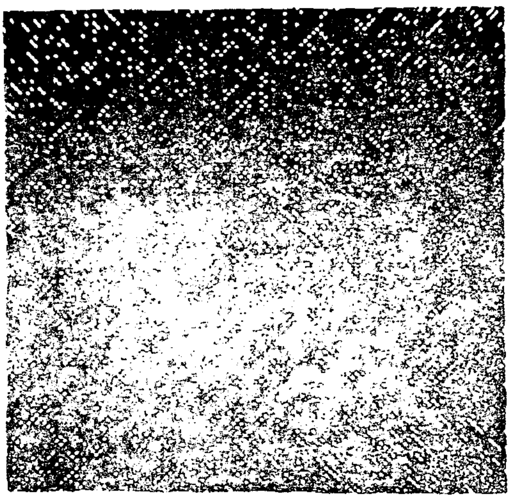

그림 3

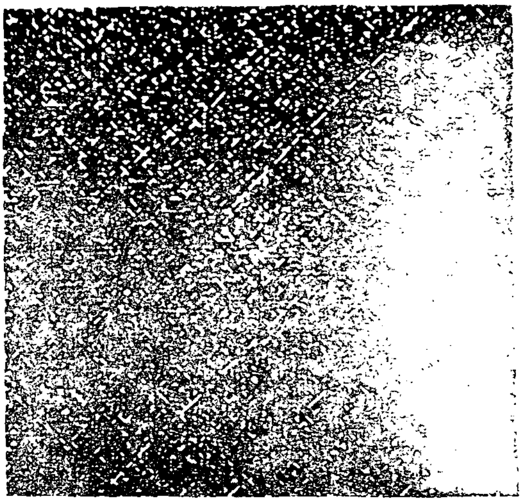

그림 4

암흑속에서도 연구를 계속하였다.

그러나 x^2+x+17에서 x가 0부터 15까지의 정수를 취할 때는 이 식의 값은 모든 素數이지만 $x=16$일 때는 素數가 아니다. 다음으로 생각한 것이 유명한 오일러의 "소수를 만드는 식" (Prime generator) x^2+x+41이다. 물론 이식도 x가 0에서 39까지 취할 때는 모두 素數이지만 $x=40$에서는 素數가 아닌 것이다. 그러나 이式에 依하여 생긴 수중에서 처음 2,398개를 取할 때는 切半이 素數이고 10,000,000까지의 數를 調査하였을 때는 47.5%가 素數인 것이다. 그러면 素數를 가장 많은 비율로 포함하고 있는 식은 과연 무엇인가? 이것 역시 다른 問題와 더불어 未解決의 問題인 것이다.

4. 素數는 無限히 많은가?(素數의 無限性)

수가 점점 크짐에 따라 素數의 密度가 희박하여 지지만 제일 큰 素數는 없다. "素數의 無限性"에 關하여는 이미 2000년 전에 유크리트(Euclid)에 依하여 證明되었다.

그는 이것을 귀류법으로 증명하였다. 만약 素數가 有限이라면 그 數가 아무리 많더라도 p_1, p_2, ……, p_n로 모두 나타낼 수 있다. 지금 새로운 수

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

을 생각하여 보자. 이 수는 두가지의 가능성을 가지고 있다. 즉 素數이던지 合成數인 것이다. 만약 K가 素數라면 K는 p_1, p_2, ……, p_n의 어느 것보다도 크다. 그러면 이것은 素數가 p_1, p_2, ……, p_n밖에 없다는 데 모순이므로 素數는 아니다. 그러면 K가 合成數라고 하자. 그러면 K는 素數의 곱으로 나타낼 수 있다. 그런데 K는 p_1, p_2, ……, p_n의 어느 것으로 나누어도 1이 남으므로 K는 p_1, p_2, ……, p_n의 곱으로는 나타낼수 없게 된다. 따라서 p_1, p_2, ……, p_n 이외에 또 다른 素數가 필요하게 된다. 그러므로 素數가 有限이라는 데 모순이다. 따라서 素數는 無限이다.

5. 소수를 만들어 내는 공식은 없는가?

그러면 이렇게 무한한 素數의 일부분이라도 찾아내는 공식은 없을가? 즉 素數 全體는 나타내지 못하더라도 어떤 공식에 어떤 數를 代入함으로 素數가 되는 方法은 없을가?

여기에서 p_1, p_2, ……, p_n가 모두 素數일 때도

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

또한 素數일 것이라는 것이다. 이것은 $p_1, p_2, \cdots, p_n$가 처음 다섯개의 소수를 取할 때는 성립하지만

$$K=2\cdot3\cdot5\cdot7\cdot11\cdot13+1=30031$$

이 될 때는 이 수는 59로 나누어 지므로 이 예상은 무너진 것이다. 그러면 달리 소수를 만들어 내는 공식이 없을가?

실로 여러해동안 많은 수학자들이 이러한 공식을 찾아내려고 무던히 노력하였다. 그러나 여기서 알수 있는 것은 이러한 식은 일반적인 대수식으로 될 수는 없겠다. 왜냐하면 대수식

$$P=a_0x^n+a_1x^{n-1}+\cdots\cdots\cdots+a_n \quad (\text{단 } a_0\fallingdotseq 0)$$

가 x에 적당한 수를 代入하므로서 素數를 만든다고 할 때, 이중 次數가 가장 낮은 항의 계수를 a_i라 하자. 그러면 $x=a_i$를 대입하였을 때, 이 식의 값은 a_i로 나누어 진다 따라서 대수 식으로 나타낼 수는 없다. 그러면 다른 어떤 공식이 없는가?

17세기에 페르마(Pierre Fermat)는 n이 자연수일 때

$$F_n=2^{2^n}+1$$

은 素數라고 하였다. (이러한 수를 "페르마의 수"라고 한다.) 여기서 $F_1=1$, $F_2=17$, $F_3=257$, $F_4=65,537$로서 素數인 것이 모두 밝혀졌다. 그리고 이 수는 n이 크짐에 따라 너무나 빨리 크지므로 $F_5=4,294,967,297$이 素數가 아니라는 것을 1732년 오일러가

$$F_5=641\times6,700,417$$

로 素因數分解(自然數를 素數의 곱의 꼴로 나타내는 것) 할 때까지는 아무도 그것을 證明할 수 없었다. 그러나 최근에는 이것을 합동식의 개념을 쓰서 더욱 간단히 증명하였다.[3] 그리고 계속하여 (1880년 이후) n이 6, 7, 8, 9, 11, 12, 18, 23, 36, 38, 73일 때 F_n가 合成數라는 것이 밝혀 졌다.

다음은 19世紀 前半에 數學者들은 $n/(\ln n)$의

값은 n까지의 素數의 個數와 비슷하다는 실험식을 만들었다. (이것을 "素數의 定理"라고 한다.) 이 식은 n이 크짐에 따라 n까지의 素數의 正確한 個數에 接近한다는 것도 1869 년 J. Hadamard와 C. de la Vallée-Poussin이 각각 따로히 Riemann의 ζ函數를 利用하여 證明하였다. [4]

즉 $\pi(n)$을 n까지의 素數의 個數라 하면

$$\lim_{n\to\infty}\frac{\pi(n)\ln n}{n}=1$$

즉 $n\to\infty$ 일 때 $\pi(n)\approx\frac{n}{\ln n}$

그러나 이 식은 素數를 만들어 내는 공식도 아니며 또한 素數의 個數를 나타내는 近似式에 지나지 않는 것이다.

그러면 人間이 구한 素數중 가장 큰 것은 얼마인가? 앞서 전자계산기로 9천만개의 素數를 구하였다고 하였다. 이 素數의 자리수는 약 100자리가 된다고 한다. 현재 알고 있는 가장 큰 素數는 1963 년 Illinois大學校의 전자계산기로 찾아낸 $2^{11213}-1$로 알고 있다. 이 수의 자리수는 3,376 자리가 된다고 한다.

6. 그러면 어떻게 하여 素數인지 아닌지 判定할 수 있는가? (任意의 數의 素數性)

전자계산기가 나오기 전에는 6,7 자리의 수의 素數性"(소수인지 아닌지)을 계산하는 데도 1주일 이상 걸렸으며 그것도 실로 부정확하였다. 오일러도 1,000,009가 素數라고 하였으나 (이때 오일러의 나이는 70이였고 장님이였을 때다.)이것은 그후에 293×3,413으로 素因數分解되는 것이 밝혀 졌다.

페르마는 100,895,169의 素數性에 關한 質問을 받았다고 한다. 그러나 그는 실로 오랜 세월을 두고 계산한 끝에 898,423×112,303으로 소인수분해되는 것을 알아내었다.

1874 년 W. Stanley Jevons는 "8,616,460,799는 어떤수로 素因數分解되는가?"라는 問題를 그의 著書 "*Principles of Science*" (科學의 原理)속에 넣었다. 그러나 여기에 關한 답변은 오늘날 전자계산기가 두 素數 96,097와 89,681의 곱으로 나타낼 때까지 아무도 알아내지 않았다.

다음으로 유명한 식이 p가 素數일 때

$$M_p=2^p-1$$

은 素數가 된다는 것이다. 여기서 M_p를 "Mersenne의 數"라고 한다. Marin Mersenne는 17세기의 불란서 신부로서 페르마, 파스칼등 여러 수학자와 친하게 지내면서 이들 數學者들의 書信交換을 맡아하였다. 그도 물론 數學에 있어서는 아마튜어였다. 그는 다시 1644 년 p가 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257일 때 M_p가 素數라고 고쳐서 발표하였다. 그는 정직하였기 때문에 자기가 풀어보지 않은 문제는 옳다고 주장하지 않았다고 한다. 그러나 이 외에도 M_{61}이 소수라는 것을 1880년에 밝혀졌으며, 그가 素數라고 한 M_{67}과 M_{257}은 실로 300 년 동안이나 素數로 인정되었지만 1903년 뉴욕에서 열린 美國數學會(AMS)에서 Frank Nelson Cole이 M_{57} 두수의 곱

193,707,721×716,838,257,287

로 素因數分解하였으며, 1931년에 D.H. Lehmer은 M_{257} 소수가 아니라는 것을 증명하였다. 여기서 재미나는 이야기는 Cole이 이것을 발표할 때 말한 마디하지 않았다는 것이다. 그러나 그후 Bell이 그에게 이것을 푸는데 얼마마한 시간이 걸렸냐고 물었을 때 3년동안의 일요일을 모두 소비했다고 대답하였다. 여기서 잠시 Bell이 쓴 原文을 그대로 옮겨 보겠다. [5]

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 andience 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."

다시 原來의 問題로 돌아가서 어떤수 n의 素數性을 알아내는 간단한 방법은 없을가? 물론 素數의 定義에 依하여 n 보다 작은 數로 전부 나눠보면 되겠지만, 실로 어마어마하게 큰 수일 때는 이것은 도저히 불가능한 것이다. 물론 電子計算機는 人間의 두뇌로 할 때 보다는 빨리해 나가지만 그렇다고 과거보다 쉬운 方法을 考案한 것은 아니다. 실제 n이 합성수인지 아닌지 판정할 때는 $[\sqrt{n}]$ 까지의 素數로 나누어 보면 되겠다. (여기서 $[\sqrt{n}]$ 는 $\sqrt{n}$ 을 넘지 않는 整數) Wilson (1741~1793)은 p가 素數가 되기 위한 *必要充分條件*은

$$(p-1)! \equiv -1 \pmod{p}$$

이라고 하였다. (이것을 "Wilson의 判定式"이라 한다.) 그러나 이것은 $[\sqrt{n}]$까지의 素數로 나누어 보는 것보다 시간이 적게 걸린다고는 할 수 없다.

7. 2보다 큰 모든 짝수는 두 素數의 合으로 나타내어 지는가? (Goldbach의 예상)

1742년 7월 7일 Christian Goldbach (1690~1764)는 오일러에게 "6보다 큰 자연수는 3개의 素數의 合으로 나타내어진다"고 하였다, 여기에 대하여 오일러는 같은 달 30일에 "모든 짝 수는 두 素數 (반드시 두 素數가 다를 필요는 없다)의 合으로 나타낼 수 있다." 고 하였다. 즉 $4=2+2$, $6=3+3$, ……, $18=11+7$. 이것을 "Goldbach의 예상"이라고 한다. 그러나 이 문제를 해결하기 爲한 최근의 많은 수학자의 연구와 發展에도 불구하고 아직 이 문제에 대한 一般解는 찾지 못하였다. [6]

단지 $n<10^5$인 n에 對하여서는 1940년 N. Pipping이 밝혀냈으며 문제는 좀 다르지만 I.M. Vinogrdov는 "充分히 큰 홀수는 3개의 素數의 合으로 나타낼 수 있다"는 것을 밝혔다.

8. 모든 合成數는 一意的으로 素因數分解되는가?

이것을 "整數論의 基本定理"라고 한다. 이 定理의 證明은 數學的歸納法으로 하겠다. [7]

우선 모든 수는 素因數分解된다는 것을 證明하자. 어떤 수 a가 素因數分解된다는 것을 $P(a)$라고 하자. a가 1이거나 素數일 때는 $P(a)$가 明白하다. a가 合成數이면 a는 1과 a 외에 約數 b를 가지게 되므로 $a=bc$, $b<a$, $c<a$이다.

지금 歸納法의 假定에 依하여 $P(b)$ 및 $P(c)$의 成立을 假定할 수 있으므로 b 및 c는 素因數分解

$$b=p_1p_2\cdots\cdots p_r,\quad c=q_1q_2\cdots\cdots q_s$$

가 가능하고, 따라서

$$a=bc=p_1p_2\cdots\cdots p_sq_1q_2\cdots\cdots q_r$$

와 같이 素因數分解된다,

다음 이의 一意性을 證明하려면 두가지로 素因數分解되었다고 假定하면,

$$a=p_1p_2\cdots\cdots p_m=q_1q_2\cdots\cdots q_n.$$

p_1은 $a=q_1q_2\cdots\cdots q_n$을 나누므로 p_1은 p_i중 적어도 하나를 나눌수 있다. 따라서

$$p_1a=q_i$$

그런데 p_1, q_i는 모두 素數이므로 $a=1$ 즉 $p_1=q_i$이다 $q_1q_2\cdots\cdots q_n$의 順序를 바꾸어서 q_i가 맨앞에 나오도록하고 p_1 및 q_i을 簡約하면,

$$p_2p_3\cdots\cdots p_m=q_2'q_3'\cdots\cdots q_n'.$$

여기서 q_i'는 q_i의 순서를 바꾼 것을 표시한다. 이러한 것을 繼續하면 兩邊중에 한번은 素因數가 없게 된다. 이 때 다른 邊에도 素因數가 없게 되므로 $m=n$. 즉 한邊의 素因數들의 順序를 적당히 바꾸면 다른邊의 素因數分解와 一致한다. 따라서 모든 合成數는 一意的으로 素因數分解가 가능하다.

9. 여러가지 재미있는 素數

英國의 Puzzle 전문가 Henry Ernest Dudeney

는 그의 著書 "*The Canterbury Puzzles*" (캔터베리의 수수께끼, 1907) 속에 11은 숫자 1만으로 된 唯一한 素數라고 하였다. 그리고 그는 3개부터 18개까지의 1로만 된 자연수를 모두 합성수로 나타내었다. 과연 더 많은 1을 반복하여 쓸 때도 모두 合成數가 될가? 이 問題에 對하여 Oscar Hope 라는 한 讀者는 19개의 1만으로 된수 1,111,111,111,111,111,111은 소수라는 것을 밝혔다. 그후 계속하여 23개의 1로 된 자연수도 素數인 것을 알았다. 그리고 숫자 1의 개수가 素數가 아니면 그 自然數는 합성수라는 것도 밝혔다. 그리고 29개, 31개, 37개, 41개, 43개, 53개, 61개, 73개의 1로된 自然數는 모두 合成數라는 것도 알았다. 아직 47개의 1로 된 수가 素數라는 것은 말하지 않았으며 또한 미해결의 問題는 이러한 數가 無限히 계속될 것인가? 하는 문재이다.

그외에 소수로서 재미나는 수는 909,090,909,090,909,090,909,090,909,091 이다.

10. 素數의 領域을 바꾸자.

다시 우리는 처음으로 돌아가서 素數의 領域을 바꾸어 보자.[8]

우리는 이제까지 素數를 自然數全體의 集合 N 內에서만 생각하였는 데, 이것을 다음과 같은 집합을 領域으로 할 때는 어떻게 될가?

E={1과 2의 양의 배수}

즉 E={1, 2, 4, 6, 8, 10,……}으로 주어 졌을 때는 이제까지 생각하였던 素數의 理論들은 어떻게 될가?

10.1 E에서 素數란 무엇인가?

여기서는 n을 自然數라 할 때 $4n-2$로 표시되는 數는 모두 素數가 되겠다. 왜냐하면 6은 N에서는 3×2로 분해 될 수 있지만 E에서는 3이라는 수를 포함하고 있지 않기 때문에 분해할 수 없다. 따라서 $4n-2$로 표시되는 수는 모두 素數이고 n번째 素數는 바로 $4n-2$인 것이다. 여기서 N의 元素 n을 쓰지 않고, E의 元素를 써서 나타낸다면 e를 1이 아닌 E의 원소로 할 때 $2e-2$로 표 시되는수는 모두 素數가 되겠다.

10.2 쌍둥이 素數란 무엇인가?

N에서 우리는 그 차가 2인 두 素數를 쌍둥이 素數라 하였다. 그러면 E에서는 인접한 素數끼리의 차가 4이므로 이 정의를 그대로 쓴다면 쌍둥이 素數는 하나도 없다고 하겠다. 그리하여 N에서 쌍둥이 素數의 정의를 "어떤 합성수의 바로 앞의 數와 바로 다음의 數가 素數일 때 이 두 素數 쌍둥이 素數라 한다"면 E에서 모든 素數는 $4n-2$, 또는 $4n+2$로 표시되므로 合成數 $4n$의 앞뒤에 있게 된다. 따라서 모두 쌍둥이 素數라고 할 수 있다.

10.3 素數의 密度는 어떠한가?

E에서는 素數의 密度는 항상 一定하며 素數의 個數와 合成數의 個數는 언제나 꼭 같다. 그리고 모든 素數를 포함하는 식은 $4n-2$로 표시할 수 있다.

10.4 素數 無限性

이것은 $4n-2$에서 $n\to\infty$에 따라 얼마던지 많은 素數를 만들 수 있다.

10.5 素數를 만드는 公式

n의 모든 값에 對하여 $4n-2$는 E에서 素數가 되었다. 또 E에서 素數와 合成數의 個數는 같다고 하였다. 그러면 E의 원소 e까지의 素數의 個數는 얼마나 될가? 이것은

$$\pi(e)=\left[\frac{e+2}{4}\right]$$

로 표시할수 있다. 즉 $\pi(1)=0$, $\pi(2)=1$, $\pi(4)=1$, $\pi(6)=2$, $\pi(8)=2, \cdots$, $\pi(18)=5, \cdots$.

10.6 素數의 判定

이것도 너무나 간단하다. 2로 나누었을 때 E내에서 나누어 떨어지면 合成數이고 그렇지 않으면 素數이다. p가 E내에서 素數가 되기 爲한 필요충분조건은 $p\equiv 2 \pmod 4$이다.

10.7 E에서 Goldbach의 豫想

여기서 문제가 되는 것은 홀수와 짝수의 정의라 하겠다. N에서 우리는 2로 나누어지는 수를

"짝수" 그렇지 않는 수를 "홀수"라 하였다. 그러면 같은 이론으로 E에서도 2로 나누어 떨어지는 수는 짝수라 하겠고, 그렇지 않는 수를 홀수라 하겠다. 따라서 E에서 합성수는 모두 짝수가 되겠고 홀수는 모두 素數가 되겠다. 따라서 짝수는 모두 $4n$으로 나타내어 진다. 여기서

$$4n=(4n-2)+2$$

로 두 素數의 합으로 표시할 수 있다. 즉

$4=2+2,\ 8=6+2, \cdots\cdots,\ 24=22+2, \cdots\cdots.$

여기서 10.2를 다시 한번 살펴보면 N에서 어떤 素數의 바로 다음의 홀수가 素數일 때 이 두 素數를 쌍둥이 素數라 한다면 E에서도 역시 같은 결과가 나온다.

10.8 素因數分解의 一意性을 성립하는가?

N에서는 항상 一意的으로 素因數分解되었지만 E에서는 성립하지 않는다.

우선 $4=2\times 2,\ 8=2\times 2\times 2,\ 12=6\times 2, \cdots\cdots$ 로 一意的으로 素因數分解되지만 36은

$$36=18\times 2=6\times 6$$

으로 素因數分解되어 素因數分解의 一意性이 成立하지 않는다.

一般的으로 k, n가 2이상의 자연수이고 p_m이 N에서 홀수인 素數일 때

$$2^k \prod_{m=1}^{n} p_m$$

으로 표시되는 E의 모든 數는 一意的으로 素因數分解되지 않으며, 또 이 때에 限한다.

10.9 또 다른 領域에서는 어떠한가?

이때까지 우리들은 領域을 E로 하였으나,

T={1과 3의 모든 양의 배수}

로 할 때, 즉 T={1, 3, 6, 9,……} 로 할 때는 어떻게 될가? 여기서는 問題로만 題示하겠다.

1. T에서 素數는 무엇인가?
2. T에서 홀수는 어떤 數인가? 또 짝수는 어떤 數인가? 그러면 이정의에서 쌍둥이 素數는 어떻게 정의할 것인가?
3. T에서 素數의 密度는 어떻게 되는가? 또 모든 素數를 나타내는 式은 있는가? 있다면 어떤 式인가?
4. T에서도 무한히 많은 素數가 있는가? 이것은 쉽게 증명되는가?
5. T에서 素數를 만드는 公式은 있는가?
6. T에서 任意의 數의 素數性을 判定할 수 있는가?
7. 문제 2에서 정의한 T의 모든 짝수에 對하여 Goldbach의 예상은 성립하는가
8. T에서 合成數는 모두 素因數分解되는가? 또 一意的인가?
9. 또 다른 領域에서 素數의 理論은 어떻게 되는가?
10. 만약 영역 E와 T에서 1을 제외한다면 이 理論은 어떻게 되는가? 素數는 어떻게 定義하겠는가? 지금까지 E와 T에서 素數라고 한 것을 素數라고 할 수 있는가? 또 合成數는 어떻게 되는가?

11. 結 論

이제까지 우리들은 素數에 關한 여러가지 問題를 모두 다루어 보았고, 未解決의 問題도 잠간 훑어 보았다. 그리고 電子計算機가 얼마나 人間의 勞力을 덜어주는가 하는 것도 살펴보았다.

素數에 關한 理論은 대체로 어렵지만, 여기에 紹介한 정도는 能히 高等學校 學生들이 理解할 수 있겠고, 또 어떤 問題는 數學을 全혀 배우지 않은 사람도 理解할 것으로 본다.

또 素數에 關한 未解決의 問題는 學生들에게 어렵겠지만, 이것을 素數의 領域을 바꿈으로서 쉽게 說明하겠고 또한 풀이도 求할 수 있겠다. 그리하여 이것은 學生들에게 未解決의 問題가 무엇인지 아리켜 주는 데도 便利할 것이다. 그러면 이제까지 열거한 內容이 數學敎育에 直接 連結될 것을 빌며 이만그친다.

(서울大學校師範大學助敎)

參 考 文 獻

[1] Kenneth P. Swallow: "*The Factorgram.*" The Mathematics Teacher, Vol. 48. No. 1. NCTM, Jan. 1955. pp. 13—19.

[2] Martin Gardner: "*The Remarkable Lore of*

the *Prime Mumbers.*" Scientific American, Vol. 210. No. 3. Mar. 1964. pp. 120—128.
[3] SMSG: "*Essays on Number Theory.*" Vol. 1. Yale University Press 1960.
[4] David Hawkins: "*Mathematical Sieves.*" Sientific American, Vol. 204. No. 12. Dec. 1958.
[5] Eric Temple Bell: "*Mathematics, Queen and Servant of Science.*" New York, McGraw-Hill 1951. pp. 229—236.
[6] Howard Eves: "*Introduction to the History of Mathematics.*" rev. ed. New York, Holt, Rinehart & Winston. 1964. p. 149.
[7] G. Birkhoff & S. Maclane; "*A Survey of Modern Algebra.*" third ed. New York; Macmillan. 1964.
(한글번역판) 尹甲炳外 3人譯: **"現代代數學槪論."** 初版 서울; 文運堂. 1962. pp. 22—23.
[8] Stephen I. Brown: "*Of 'prime' concern: What domain?*" The Mathematics Teacher, Vol. 58. No. 5. NCTM. May 1965. pp. 402—407.

—— ◇ ——

全國 數學敎育硏究大會 硏究發表 案內

1966年度 全國數學敎育 硏究大會의 硏究發表를 希望하는 會員 여러분은 아래와 같은 要領으로 準備하여 주시기 바랍니다.

1. **申請期間**: 1966年 7月 15日까지 (期日嚴守)
2. **申請樣式**: 아래와 같은 樣式으로 200자 原稿紙 3枚(600字) 以內의 內容要約을 提出할 것.

發表 希望 分科名 〔 〕 發表 所要時間〔 分〕
姓　名
勤務處
住　所
論文題目
內容要約 (600字 以內) ……………………………………………………………………
……………………………………………………………………………………………

3. **注意事項**:
(1) 硏究發表는 20分 程度로 끝내 주시기 바라며 얼마간의 時間의 연장을 願하는 분은 미리 알려 주시기 바랍니다.
(2) 本硏究大會에서 配布되는 제반 프린트, 인쇄물, 기타는 반드시 그중 一部를 發表當日 接受에 提出하여 주시기 바랍니다.
(3) 發表를 申請하신 때는 봉투의 表面에 "硏究發表"라 朱書하시고 大會準備委員會 連絡處로 送付하시기 바랍니다.
(4) 大會準備委員會의 連絡은 可及的 書面으로 하여 주시고, 返信을 要하는 경우에는 住所를 記入한 返信用 봉투를 同封하여 주시기 바랍니다.
4. **大會準備委員會 連絡處**:
(1) 釜山大學校 工科大學　李 忠 杰
(2) 서울大學校 師範大學　崔 英 瀚

1966 년 6월 　일

全 國 數 學 敎 育 硏 究 大 會 準 備 委 員 會