한국수학사학회지 제21권 제3호(2008년 8월), 113 - 126

ABC추측의 발전과 다항식 반복의 연구1)

한남대학교 수학과 최은미
emc@hnu.kr

abc추측의 역사적 발전 과정과 페르마정리와의 관계를 살펴보며, abc추측이 디오판토스방정식풀이와 이항다항식 $f(x)=x^n-b$ 반복의 불변성연구에 응용되는 면을 연구한다.

주제어: abc추측, 디오판틴방정식, 다항식반복

1. 서론

방정식 $x^n+y^n=z^n$ $(n>2)$은 0이 아닌 정수근을 갖지 않는다는 페르마(P.Fermat, 1601-1665)의 마지막정리는 1995년에 와일즈(A.Wiles, 1953-)에 의해 증명될 때까지 350년가량을 미해결 문제로 있었다. 페르마정리의 증명을 향한 노력은 변수 3개인 디오판토스방정식의 일반해를 찾는 방향으로 전개되었으며, 이 과정에서 나타난 문제들은 abc추측으로 집약되었다. 실제로 abc추측이 성립하면 페르마 정리가 쉽게 증명된다. 이제 페르마 정리는 증명되었지만, abc추측은 여전히 중요한 위치에 있다. 이는 abc추측이 정수론의 여러 중요한 문제들과 동치관계이기 때문이다. 한편, 이항다항식 $f(x)$의 특별한 어떤 성질이 다항식 반복(iteration)에서도 여전히 유효할 것인가 하는 불변성 연구는 많은 사람들의 관심을 받아왔다. 예컨대 $f(x)$가 기약성이나 분해성을 가질 때 $f(x)$의 m번 반복에서 기약성 혹은 분해성이 유지될 것인가 하는 문제인데, 이 때 abc추측을 바탕으로 한 디오판토스방정식 풀이 이론이 큰 역할을 한다.

이 논문에서는 abc추측의 역사적 발전 과정을 통해 페르마 정리와의 관계를 살펴보며, abc추측이 디오판토스방정식 풀이와 이항다항식 $f(x)=x^n-b$의 반복 $f_m(x)$에서 불변성연구에 응용되는 면을 연구하려고 한다.

1) 이 논문은 2007년 한남대학교 교비지원으로 연구됨.

2. 디오판토스방정식에서의 ABC 추측

2-1. 페르마정리와 함수체에서의 페르마정리

$n>2$일 때 방정식 $x^n+y^n=z^n$은 단지 자명한 근을 갖는다는 페르마의 주장은 결국 와일즈에 의해 증명되었다. 알려져 있지 않은 페르마의 증명 방법이 와일즈의 것과는 상당히 다를 것이라고 많은 사람들이 추측하고 있는데, 이는 와일즈의 증명법이 지난 350년 실패의 기간 동안 축척된 수많은 수학자들의 연구 위에 만들어졌기 때문이다. 더욱이 페르마가 정말 증명을 했었을까하는 의구심과 더불어 그가 실수한 것일지 모른다고 생각하는 학자들도 있다. 페르마의 마지막방정식은 디오판토스방정식의 한 종류이다. 알렉산드리아의 디오판토스(Diophantus, 200-284)의 이름을 딴 것으로서 그의 저서 아리스메티카(Arithmetica)에서 다루었다. 페르마는 아리스메티카의 라틴어 번역본을 공부했으며 책의 여백에 노트를 했다. 페르마 사후 그의 아들은 아리스메티카의 개작을 출판하면서 페르마의 노트를 부록에 첨가하였다[12].

페르마의 마지막정리를 향한 와일즈의 증명은 Shimura-Taniyama-Weil 추측에 대한 탐구로 이어졌으며, 3변수 디오판토스방정식의 일반화를 유도하는데 큰 도움을 주었다. 여기서 중요한 열쇄는 abc추측으로 요약되었다. a,b,c가 다항식일 때 Mason정리를 사용하여 페르마의 마지막정리가 쉽게 증명되어짐에 착안하여, 1985년에 프랑스의 Oesterle[10]와 스위스의 Masser[8]는 Mason정리를 정수 환 위로 확장하려는 과정에서 abc추측을 독립적으로 제안하였다.

페르마 정리의 증명이 계속 난항을 겪는 과정에서, 페르마방정식을 다항식의 방정식으로 바꾸어서 해결해보려는 시도가 있었다. 정수 체계에서 다루기 힘든 문제들이 함수체(function field)에서는 비교적 쉽게 해결되어지는 일이 종종 벌어진다. 실제로 1851년의 J. Liouville(1809-1882)은 다항식에 관한 페르마정리를 증명했는데, 그의 증명은 적분 개념을 포함하여 매우 복잡한 형태로 전개된다[5]. 최근 50여 년 전부터 다항식에 관한 페르마 정리의 증명은 다음과 같은 형태로 많이 소개되었다.

다항식에 관한 페르마의 마지막정리: $x=x(t)$, $y=y(t)$, $z=z(t)$는 서로소인 다항식으로서 표수 0인 대수적 폐체에서 계수를 갖는다고 하자. 그러면 페르마방정식

$$x^n+y^n=z^n \qquad \cdots \text{ (FLE)}$$

는 $n\geq 3$일 때 근을 갖지 않는다.[2)]

(FLE)가 근 x,y,z를 갖는다고 하자[5]. x,y,z가 공약수를 가진다면 그것으로 x,y,z를 나누어서 서로소가 되도록 만들 수 있으므로, 여기서는 x,y,z가 서로소인 근이라고 가정한다. 식(FLE)을 미분하면

2) $n=2$이면 방정식 $x^n+y^n=z^n$은 근을 가지며, 가령 $(2t)^2+(t^2-1)^2=(t^2+1)^2$가 된다.

$$nx^{n-1}x' + ny^{n-1}y' = nz^{n-1}z',$$

즉

$$x^{n-1}x' + y^{n-1}y' = z^{n-1}z'$$

를 얻는다. 식(FLE)에 y'을 곱하고, 위 식에 y를 곱하여 연립하면

$$x^{n-1}(xy' - yx') = z^{n-1}(zy' - yz')$$

을 얻는다. 즉 x^{n-1} 은 $z^{n-1}(zy' - yz')$ 을 나눈다. 만약

$$zy' - yz' = 0$$

이라면

$$(y/z)' = \frac{y'z - yz'}{z^2} = 0$$

이 되어

$$y = kz \quad (k : \text{상수})$$

인데, 이는 x,y,z가 서로소라는 가정에 모순이다. 그러므로 $zy' - yz' \neq 0$ 이다. 또한 $\gcd(x,z) = 1$ 이므로 식 $x^{n-1} \mid z^{n-1}(zy' - yz')$ 로부터

$$x^{n-1} \mid (zy' - yz')$$

이다. 그런데 $\deg(y') = \deg(y) - 1$이고 $\deg(z') = \deg(z) - 1$이므로 차수를 비교하면

$$\deg(x^{n-1}) \leq \deg(zy' - yz')$$

즉

$$(n-1)\deg(x) \leq \deg(zy' - tz') \leq \deg(y) + \deg(z) - 1$$

가 된다. 양변에 $\deg(x)$를 더하면

$$n\deg(x) \leq \deg(x) + \deg(y) + \deg(z) - 1$$

가 된다. 이 식은 대칭의 형태이므로 이와 유사하게

$$n\deg(y) \leq \deg(x) + \deg(y) + \deg(z) - 1$$
$$n\deg(z) \leq \deg(x) + \deg(y) + \deg(z) - 1$$

를 만들 수 있다. 따라서 위의 식을 모두 합하면

$$\begin{aligned} n(\deg(x) + \deg(y) + \deg(z)) &\leq 3(\deg(x) + \deg(y) + \deg(z) - 1) \\ &< 3(\deg(x) + \deg(y) + \deg(z)) \end{aligned}$$

즉,

$$n < 3$$

이다. 그러므로 $n \geq 3$일 때 방정식(FLE)은 근을 가지지 못한다.

다항식 환에서의 페르마정리에 대한 위의 증명법을 일반화하여 정수에서의 페르마정리로 확장하려는 여러 노력들 중에, 1984년의 Mason의 방법은 페르마정리 증명과 디오판토스방정식 풀이에 새로운 전기가 되었다.

Mason정리:[7] $a = a(t)$, $b = b(t)$, $c = c(t)$가 복소수 계수를 갖는 서로소인 다항식들로서 $a + b = c$ 를 만족한다고 하자. 그러면 다음이 성립한다.

$$\max(\deg(a),\deg(b),\deg(c)) < \#\{\alpha \mid abc(\alpha)=0\}$$

복소수 계수를 갖는 다항식 P의 서로 다른 근의 개수를 P의 radical이라 부르며, 기호 $N_0 = N_0(P)$로 나타내는데, 이를 사용하면 다음과 같은 부등식이 된다.

$$\max(\deg(a),\deg(b),\deg(c)) \le N_0(abc)-1$$

이는 다항식에 관한 abc정리라고 불리며, 다항식의 페르마정리 증명에 사용된다. 표수 0인 대수적폐체에서 정의된 서로소인 다항식 $x=x(t)$, $y=y(t)$, $z=z(t)$이 $x^n+y^n=z^n$ $(n\ge 3)$를 만족한다고 하자. x,y,z중에서 최대 차수인 다항식을 x라 하면, Mason 정리에 의해 다음의 부등식이 성립한다.

$$n\deg x = \deg x^n < \#\{\alpha \mid (xyz)^n(\alpha)=0\} = \#\{\alpha \mid (xyz)(\alpha)=0\} \le \deg xyz \le 3\deg x$$

따라서 $n<3$ 이 되어, 페르마정리가 간단히 증명된다.

2-2. abc추측을 향한 발전 과정들

Mason정리가 페르마 정리에 효과적임을 입증된 후, 정수 체계로 전환시키려는 추측과 노력이 이어졌다. 결론으로 말하면, 이것은 여전히 추측으로 남아있다. 대수학의 기본정리에서 기약 다항식의 역할은 정수에서의 소수로 비견되므로, Mason정리는 정수 계에서 다음과 같은 형태로 표현될 수 있을 것이라고 추측하였다[5].

추측 1. 만약 a,b,c가 서로소인 정수들로서 $a+b=c$를 만족하면 a (또는 b, c)의 소인수의 개수 (중복도허용) 는 abc의 소인수의 총 개수보다 작다.

반례: 수없이 많은 반례를 찾을 수 있다: $1+1=2$, $1+3=4$ 또는 $1+7=8$. 더욱 심각한 경우는 Mersenne 소수의 경우로서 2^n-1이 소수이면 '추측 1'은 $n<1+1$이라는 엉뚱한 결과를 만들어낸다.

한편 $\log p$를 곱하여 소수를 세는 방법이 해석적 정수론에서 이용되어 왔다. $a(t)$의 차수에 대응하는 것으로서, 정수 $a=\prod_p p^{e_p}$ 에 적용할 수 있는 방법은 a의 소인수의 개수 $\sum_p e_p$가 아니라 오히려 $\sum_p e_p \log p$ 가 적절할 것이라는 생각이었다. 그런데

$$\sum_{p|a} e_p \log p = \sum_p \log p^{e_p} = \log \sum_p p^{e_p} = \log a$$

이므로 다항식 곱 $a(t)b(t)c(t)$의 서로 다른 인수들의 개수는, 정수곱 abc에서 $\sum_{p|abc}\log p$로 대체할 수 있다. (여기서 합 $\sum$은 abc의 서로 다른 소인수 p에 대해 택한다.) 양변에 지수함수를 적용하면 다음과 같은 추측을 얻게 된다[5].

추측 2. a,b,c가 서로소인 정수들로서 $a+b=c$를 만족하면 다음이 성립한다.

$$\max\{a,b,c\} \le \prod_{p|abc} p \quad (p \text{ 소수})$$

반례: $3+7=10$ 에서 $10<\prod_{p|3\cdot 7\cdot 10} p = 3\cdot 7\cdot 10$ 이지만, 항상 성립하지는 않는다. $1+8=9$ 일 때 $1\cdot 8\cdot 9=2^3 3^2$이므로 $\prod_{p|72} p=6<9=\max\{1,8,9\}$이며, $32+49=81$일 때 $32\cdot 49\cdot 81=2^5 3^4 7^2$이므로 $\prod_{p|abc} p=42<81$이다. 또한 $3+125=128$일 때 $2\cdot 3\cdot 5<128$이다. 그 외에도 여러 개의 반례가 있다.

Mason정리에 대응하는 결과를 정수 체계에서 적절한 형태로 만들어보려는 노력들이 실패로 돌아갔지만, 수치해석적인 연구를 통해 점점 결론에 근접해 간다는 믿음이 커졌다. 실제로 추측 2의 반례들에서 발생한 문제점을 해결하기위해, 또 다른 노력이 있었으며, 바로 여기서 abc추측을 유도하는 과정이 나오게 되었다.

2-3. Masser과 Oesterle 의 abc추측

$rad(n)$은 정수 n의 square-free 부분이라고 하자. 가령 p가 소수이면 $rad(p)=p$이며, $rad(15)=15$, $rad(16)=2$, $rad(1400)=(2)(5)(7)=70$이다. $rad(n)$은 Mason정리에서 사용한 다항식의 radical에 대응하는 개념으로 이해할 수 있다.

추측 3. 양의 정수 a, b와 $a+b=c$일 때, $c<rad(abc)$, 즉 $rad(abc)/c>1$ 이다.

그러나 위에서 소개한 여러 반례에서 볼 수 있듯이 (가령 $1+8=9$ 등에서)

$$rad(abc)<c, \quad 즉 \quad rad(abc)/c<1 \qquad \cdots \quad (1)$$

인 경우도 많이 있다. 위의 반례들의 유형을 분석한 결과, $rad(abc)/c$는 결코 커지지 않는다. 즉 $1+8=9$일 때 두 변의 비율은 9/6이며, $32+49=81$와 $3+125=128$ 일 때의 비율은 각각 27/14과 64/15가 된다. 0부터 1000사이의 모든 정수 a,b,c에 대해 비율 $c:rad(abc)$ 을 조사한 결과, 방정식 $1+2^9=3^3\cdot 19$로부터 얻어진 부등식 $\prod_{p|2^9\cdot 3^3\cdot 19} p=2\cdot 3\cdot 19<3^3\cdot 19$ 의 비율 9/2가 가장 큰 값임이 알려졌다. 그러므로 식 (1)에 9/2보다 적당히 큰 상수 (가령 5)를 곱하면 추측 3의 부등식 형태가 될 것이라고 추측했다. 그러나 이것 역시 거짓인데, $a=1$, $b=2^{q(q-1)}-1$ (q: 큰 소수) 또한 $c=2^{q(q-1)}$이면, b는 q^2에 의해 나누어져서, 식 (1)의 우변은 $\leq 2b/q$ 가 된다.

일반적으로 $rad(abc)$가 c보다 크기는 하지만, a,b를 잘 택함으로서 $rad(abc)/c$ 는 아주 작은 값이 될 수 있음이 Masser에 의해 증명되었다[8],[12]. 즉 임의의 $\epsilon>0$에 대해 $rad(abc)/c$ 가 ϵ보다 작아지는 정수 a,b를 항상 찾을 수 있다.

이제 $rad(abc)$와 c의 비율을 택하는 대신 각각 값에 대한 로그값을 택하여 분수를 만들게 된다. 정수 a,b,c로부터 만들어지는 분수 $P(a,b,c)=\dfrac{\log\max(|a|,|b|,|c|)}{\log rad(abc)}$ 을

a,b,c의 멱(power)이라 부를 때, Oesterle는 다음을 추측하였다.
Oesterle 추측: 서로소인 양의 정수 a,b,c가 $a+b=c$이면 $P(a,b,c)$는 유계이다.

그 후 많은 시행착오를 거쳐 1985년에 이르러 다음 형태의 추측이 구성되었다.
Masser-Oesterle의 abc추측: 서로소인 정수들로서 abc방정식 $a+b=c$를 만족하면, 임의의 실수 $\eta>1$에 대해 $P(a,b,c)>\eta$인 a,b,c는 유한개 존재한다.[4]

Masser는 더 일반화하여 오늘날 우리가 abc추측[3]이라고 부르는 형태를 만들었다.

abc추측 1: 임의의 $\epsilon>0$에 대해 상수 $C_\epsilon>0$이 항상 존재하여 $a+b=c$이며 서로소인 모든 정수 a,b,c에 대해 다음의 부등식이 성립한다.

$$\max(|a|,|b|,|c|) \le C_\epsilon [rad(abc)]^{1+\epsilon} = C_\epsilon \left(\prod_{p|abc} p\right)^{1+\epsilon} \qquad (p \text{ 소수})$$

만약 a,b,c가 양의 정수라면 위 부등식은 $c \le C_\epsilon [rad(abc)]^{1+\epsilon}$ 가 된다.

한편, 위의 abc추측의 형태를 다음과 같이 표현할 수 있다.
abc추측 2: ϵ은 임의의 양수라고 하자. $a+b=c$이며 서로소인 모든 정수 a,b,c가 있을 때, 비율 $[rad(abc)]^{1+\epsilon}/c$ 는 작은 상수 $k_\epsilon>0$ 에 의해 아래로 유계이다. 즉,

$$k_\epsilon < \frac{[rad(abc)]^{1+\epsilon}}{c}$$

이것은 Masser정리에 모순되는 형태로서, 만약 n이 1보다 큰 임의의 수 (심지어는 $n=1+10^{-30}$이라하더라도) 라면 $[rad(abc)]^n/c$ 는 최소값으로 접근한다.[12]

2-4. abc추측의 결과와 일반화된 페르마정리

다항식에 관한 Mason정리를 정수계에서 재구성해 보려는 첫째 의도는 정수에서의 페르마정리를 풀고자 하는 것이었다. 그러나 정수에서는 Mason정리에 대응하는 내용을 증명할 수 없는 대신, abc추측을 구성할 수 있었다. 이를 증명할 수 있다면 페르마정리는 물론 정수론에서의 여러 개의 유명한 추측들도 쉽게 해결할 수 있다.

Asymptotic 페르마정리[5]: abc추측은 충분히 큰 n에 대해 페르마정리를 유도한다. 즉, n이 충분히 클 때 $x^n+y^n=z^n$는 0이 아닌 서로소인 정수근을 갖지 않는다.

3) abc추측의 이름은 Masser와 Oesterlé가 사용한 방정식 $a+b=c$으로부터 유래되었다. 만약 $x+y=z$으로 표시하였다면 xyz추측이 되었을 지도 모른다.

$x^n+y^n=z^n$을 만족하는 서로소인 양의 정수 근 x,y,z가 있다고 가정하자. $a=x^n$, $b=y^n$, $c=z^n$라 하여 abc 방정식 $a+b=c$을 생각하면,

$$rad(x^n y^n z^n)=rad(xyz)\le xyz$$

이 된다. abc추측에 의해 임의의 $\epsilon>0$에 대해 항상 $C_\epsilon>0$ 이 존재하여

$$\max\{x^n,y^n,z^n\}\le C_\epsilon[rad(xyz)]^{1+\epsilon}\le C_\epsilon(xyz)^{1+\epsilon}$$

가 된다. 다시 말해

$$x^n\le C_\epsilon[rad(xyz)]^{1+\epsilon}\le C_\epsilon(xyz)^{1+\epsilon}$$

$$y^n\le C_\epsilon[rad(xyz)]^{1+\epsilon}\le C_\epsilon(xyz)^{1+\epsilon}$$

$$z^n\le C_\epsilon[rad(xyz)]^{1+\epsilon}\le C_\epsilon(xyz)^{1+\epsilon}$$

이 되며, 이제 각 변을 곱하여 다음의 부등식을 얻을 수 있다.

$$(xyz)^n\le\left(C_\epsilon(xyz)^{1+\epsilon}\right)^3=C_\epsilon^3(xyz)^{3(1+\epsilon)}$$

식의 양변에 로그함수를 택하면

$$n\ \ln(xyz)\le 3\ln C_\epsilon+3(1+\epsilon)\ln(xyz)$$

즉,

$$(n-3-3\epsilon)\ln(xyz)\le 3\ln C_\epsilon$$

이 된다. 그런데 $xyz\ge 2$이므로

$$n<3\frac{\ln C_\epsilon}{\ln 2}+3+3\epsilon$$

가 되어, n은 상계를 갖는다. 그런데 n이 상계보다 커지면 모순이다. 따라서 충분히 큰 n일 때 페르마방정식 $x^n+y^n=z^n$는 0이 아닌 근을 가질 수 없다.

다음의 정리[4]도 유사한 방법으로 증명할 수 있다.

정리: $n>3$일 때 방정식 $x^n+y^n=z^n$를 만족하는 서로소인 정수근 x,y,z는 많아야 유한개 존재한다. 더욱이 방정식 $x^n+y^n=z^n$, $\gcd(x,y,z)=1$이 있을 때, 항상 $N\in\mathbb{Z}$가 존재하여 $n>N$인 모든 n에 대해 단지 자명한 정수근만이 존재한다.

2007년 까지 abc추측은 증명되지 않았지만 긍정적인 결과들이 많이 발표되었으며, 실제로 $a+b=c$인 양수들에서 c는 다음의 값들에 의해 유계임이 밝혀졌다.

$$\exp(C_1 rad(abc)^{15}),\quad \exp(C_2 rad(abc)^{2/3+\epsilon}),\quad \exp(C_3 rad(abc)^{1/3+\epsilon})$$

여기서 C_1은 절대 상수이고 C_2와 C_3는 ϵ값으로 계산되는 양수이다.[14],[15]

abc추측은 일반화된 페르마방정식 $x^p+y^q=z^r(p,q,r\ge 2)$과 Catalan(1814-1894) 방정식$x^p-y^q=1(p,q\ge 2)$에도 적용되며[5], 또한 임의의 정수 A,B,C를 계수로 하는 페

4) 와일즈의 증명 이후 더 이상은 추측 (conjecture)이 아니라 정리로서 평가되어진다.

르마방정식 $Ax^p + By^q = Cz^r$ $(p,q,r \geq 2)$에도 사용할 수 있다.

Fermat-Catalan추측: 방정식 $x^p + y^q = z^r$는 양의 정수 $p,q,r > 1$이

$$\chi = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$$

의 부등식을 만족할 때, 서로소인 양수 근 x,y,z가 많아야 유한개 존재한다.

현재까지 Fermat-Catalan방정식의 정수근은 모두 10개가 알려져 있다[5] [9].

표 :	$x^p + y^q = z^r$	x	y	z	p	q	r	χ
i)	$1^p + 2^3 = 3^2$	1	2	3	p	3	2	
ii)	$2^5 + 7^2 = 3^4$	2	7	3	5	2	4	19/20
iii)	$7^3 + 13^2 = 2^9$	7	13	2	3	2	9	25/27
iv)	$2^7 + 17^3 = 71^2$	2	17	71	7	3	2	41/42
v)	$3^5 + 11^4 = 122^2$	3	11	122	5	4	2	19/20
vi)	$17^7 + 76271^3 = 21063928^2$	17	76271	210663928	7	3	2	41/42
vii)	$1414^3 + 2213459^2 = 65^7$	1414	2213459	65	3	2	7	41/42
viii)	$9262^3 + 15312283^2 = 113^7$	9262	15312283	113	3	2	7	41/42
ix)	$43^8 + 96222^3 = 30042907^2$	43	96222	30042907	8	3	2	23/24
x)	$33^8 + 1549034^2 = 15613^3$	33	1549034	15613	8	2	3	23/24

실제로 1995년 Darmon과 Granville은 Fermat-Catalan추측의 한 형태를 증명하였다.

Darmon과 Granville정리[5]: $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ 인 양의 정수 p,q,r에 대해 $x^p + y^q = z^r$를 만족하는 서로소인 세 쌍의 수 x,y,z는 유한개 존재한다.

표에서 ii)부터 x)의 경우 χ값을 구체적으로 계산할 수 있는데, 모두 1보다 작다. 한편 i)의 χ값은 p에 따라 바뀌며 $\chi = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$가 되는 최대값을 계산할 수 있다.

성질 : $\chi = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ 중에서 최대인 값은 $\frac{41}{42}$이다.

만약 $p = q = r = 2$라면 $\chi = 3/2 > 1$이다. $p = q = 2$일 때 $r > 2$라면 그 중에서 최대인 χ값은 r이 최소인 $r = 3$, 즉 $\chi = \frac{4}{3} > 1$이 된다. 그러므로 $p = 2$이고 $q,r > 2$라면

(p,q,r)	$(2,3,3)$	$(2,3,4)$	$(2,3,5)$	$(2,3,6)$	$(2,3,7)$
χ	$\chi = 7/6 > 1$	$\chi = 13/12 > 1$	$\chi = 31/30 > 1$	$\chi = 6/6 = 1$	$\chi = 41/42 < 1$

5) 큰 수를 포함하는 마지막 5개 방정식은 Beukers 와 Zagier가 컴퓨터를 사용해 알아냈다.

가 되어 $\chi<1$인 경우가 처음 나왔다. $p,q,r>2$라면, $p=q=r=3$일 때 χ는 최소값 1이다. $(p,q,r)=(3,3,4)$이면 $\chi=11/12<1$이며, $(p,q,r)=(3,4,4)$이면 $\chi=10/12<1$이다. 그러나 $10/11<11/12<41/42$이므로, 현재까지 $\chi=41/42$은 1보다 작은 최대값이다. 실제로 만약 (p,q,r)이 존재하여 $\frac{41}{42}<\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1$라고 가정하자. 그러면 반드시 $p=2$이며 $q,r\geq 3$이다. $\frac{41}{42}<\frac{1}{2}+\frac{1}{q}+\frac{1}{r}$ 과 $\frac{1}{2}+\frac{1}{q}+\frac{1}{r}<1$로부터

$$\frac{(2r)}{(r-2)}<q<\frac{(21r)}{(10r-21)}$$

을 얻게 된다. 몇 개의 r에 대해 계산하면

$r=3:\ 6<q<7$	$r=4:\ 4<q<4.421$	$r=5:\ 3.333<q<3.621$
$r=6:\ 3<q<3.231$	$r=7:\ 2.8<q<3$	$r=8:\ 2.666...<q<2.739$

가 되어, 정수 q는 존재하지 않는다. 더욱이 $r\to\infty$를 하면 $2<q<2.1$이 되어 $q\geq 3$인 정수는 존재하지 않는다. 따라서 $\frac{1}{2}+\frac{1}{3}+\frac{1}{7}=\frac{41}{42}$ 는 1 보다 작은 최대값이다.

그러면 abc추측은 Fermat-Catalan방정식에서 어떠한 역할을 하는가. $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}<1$로부터 $\frac{1}{p}+\frac{1}{q}+\frac{1}{r}\leq\frac{41}{42}$ 이 되므로, abc추측을 방정식 $x^p+y^q=z^r$ 에 적용하면

$$\max\{|x|^p,|y|^p,|z|^r\}\leq C_\epsilon\,[rad(x^py^qz^r)]^{1+\epsilon}$$

이 된다. $x,y,z>0$ 로 가정하면 $\max\{|x|^p,|y|^p,|z|^r\}=z^r$ 이다. 한편,

$$rad(x^py^qz^r)=rad(xyz)\leq xyz=(x^p)^{\frac{1}{p}}(y^q)^{\frac{1}{q}}(z^r)^{\frac{1}{r}}\leq(z^r)^{\frac{1}{p}+\frac{1}{q}+\frac{1}{r}}\leq z^{\frac{41}{42}r}$$

이므로

$$z^r\leq C_\epsilon\, z^{\frac{41}{42}r(1+\epsilon)}$$

이다. 만약 $\epsilon=\frac{1}{83}$으로 택한다면,

$$z^r\leq C_\epsilon\, z^{\frac{41}{42}r\frac{84}{83}}=C_\epsilon\, z^{r\frac{82}{83}}\quad\text{이며}\quad z^{r\frac{1}{83}}\leq C_\epsilon$$

즉, $z^r\leq(C_\epsilon)^{83}$ 이다. 다시 말해 z는 상계를 가진다. 유사하게 x,y도 상계를 가지므로, x,y,z는 유한개의 가능성(근)이 존재한다. 그러므로 다음의 정리를 유도한다.

정리. abc추측은 Fermat-Catalan 추측을 유도한다.

3장. 디오판토스방정식과 이항다항식 반복 $f_m(x)$에서 abc 추측

3-1. 디오판토스방정식 해에 관한 abc 추측

디오판토스방정식$\{p,q,r\}$: $x^p+y^q=z^r$에서 상수값 $\chi=\frac{1}{p}+\frac{1}{q}+\frac{1}{r}$는 방정식 근의 존재성을 판단하는 중요한 지표가 되며 3경우로 나누어 생각할 수 있다[6].

i) $\chi>1$이면 $\{p,q,r\}$은 $(2,2,k)$, $(2,3,3)$, $(2,3,4)$, $(2,3,5)$의 치환(permutation) 형태이다. 이 경우의 방정식은 근을 갖지 않거나 무한히 많은 근을 갖는다고 밝혀졌다. 실제로 방정식 $\{p,q,r\}$이 $\{3,3,2\}$,$\{2,3,4\}$, $\{2,4,3\}$, $\{2,3,5\}$ 일 때 근이 발견되었으며 어떤 경우에든 무한히 많은 근이 존재한다.

ii) $\chi=1$이면 $\{p,q,r\}$은 $(2,4,4)$, $(2,3,6)$, $(3,3,3)$의 치환 형태이다. 이 경우 많아야 유한개의 근을 갖는데, 가령 $\{2,6,3\}$, $\{3,3,3\}$, $\{4,4,2\}$, $\{4,2,4\}$는 근이 전혀 없으며, $\{2,3,6\}$는 Catalan방정식으로서 $3^2+(-2)^3=1$이 자명하지 않는 유일한 근이다.

iii) $\chi<1$이면 $\{p,q,r\}$의 가능성은 무한히 많다. 이 경우 방정식은 유한개의 서로소인 근을 가질 것이라고 추측되었으며(Fermat-Catalan추측), Darmon과 Granville이 1995년에 증명했다. 또한 p,q,r이 충분히 클 때는 전혀 근을 갖지 않을 것으로 추측된다. 따라서 $\{3,3,r\}(r>3)$은 유한개의 근을 가지며, 더욱이 abc추측에 의해 r이 충분히 클 때 방정식은 자명한 근 만을 갖는다.

$\chi<1$일 때가 흥미로운 경우로서 많은 연구가 진행되었다. 방정식$\{p,q,r\}$의 자명하지 않은 원시 정수근들의 집합 $T(p,q,r)$에 대해 다음이 성립한다.

정리 [3],[6]: Shimura-Taniyama추측(유리수체 위에서의 타원곡선은 modular이다)이 성립한다고 가정하자.
(1) 소수$p>13$이며 $p\equiv 1(\mathrm{mod}4)$이면 $T(p,p,2)=\varnothing$이다. (가령 $T(17,17,2)=T(29,29,2)=\varnothing$이다.)
(2) 소수 $p>13$이며 $p\equiv 1(\mathrm{mod}3)$이고 또한 p가 Mersenne가 아니면 $T(p,p,3)=\varnothing$이다. (가령 $T(13,13,3)=T(19,19,3)=T(37,37,3)=T(43,43,3)=\varnothing$이다.)
(3) 모든 $s\geq 3$에 대해 $T(s,s,4)=\varnothing$이다. 특히 $s\geq 3$에 대해 $T(s,s,s)=\varnothing$이다.
(4) $3\leq p<10^4$인 소수이면 $T(3,3,p)=\varnothing$이다.
(5) $s,t\geq 2$이고 $p\geq 3$인 소수라면 $T(3s,3t,p)=T(3s,p,3t)=\varnothing$이다.

여기서는 Shimura-Taniyama추측을 가정하였으나, 최근 Conrad, Diamond, Taylor의

연구로 인해 대부분의 경우에 그러한 조건을 필요로 하지 않게 되었다.

집합 T에 관해 다음의 결과도 알려져 있다.
(6) $r=4$ 또는 5일 때, $T(3,3,r)=\varnothing$ 이다.
(7) $p\geq 4$이면 $T(p,p,2)=\varnothing$ 이다. 특히 $t\geq 2$이면 $T(4,t,4)=\varnothing$ 이다. (가령 $T(4,4,2)=T(5,5,2)=T(6,6,2)=\varnothing$ 이다.)

3-2. 이항다항식의 불변성에서의 abc추측

다항식 $f(x)$의 m번 반복(iteration) $f\circ\cdots\circ f$를 $f_m(x)$라 하자. 그러면 $f_1(x)=f(x)$, $f_m(x)=f(f_{m-1}(x))$이며, 편의상 $f_0(x)=x$라 하자.

다항식 반복에서의 불변성(invariant) 문제가 제기되었다.
문제: 다항식 $f(x)$의 어떤 성질 P가 있어서, $f(x)$의 처음 m번 반복까지는 P가 성립하지만 그 다음 $m+1$번째 반복에서는 성립하지 않는 성질을 알아보자. 구체적으로, $f(x)=x^n-b$ ($b\neq 0$은 단원이 아님)가 K위에서 기약일 때 그것의 모든 반복들이 K위에서 여전히 기약이기 위해 K, n, b가 만족해야하는 조건을 알아보자.

정리:[2] R은 유일인수분해정역(UFD), K는 R의 분수체이며, $b_1, b_2\in R$는 서로소로서 $b=b_1/b_2\in K$ 라 하자. K에서 기약인 다항식 $f(x)=x^n-b$에 대해 $f_m(m\geq 1)$은 기약이지만, f_{m+1}는 가약이라 하자. 그러면 적당한 소인수 $p\,|\,n$와 단원 $u\in R$ 그리고 원소 $d, z, w_{m-1}\in R$ 이 존재하여 다음의 성질을 만족한다.

(1) $ud^p=b_1$

(2) $z^p=(-1)^{n^m}u\left(u^{n-1}d^{p(n-1)}w_{m-1}^n-b_2^{n^m-1}\right)$ … (2)

(3) d, w_{m-1}, b_2 그리고 z 는 R에 속하는 0이 아닌 서로소이다.

실제로 수열 $\{w_j\}$는 다음과 같이 된다.

$$w_0=-1;\ w_1=b_1^{n-1}w_0^n-b_2^{n-1}=(-1)^n b_1^{n-1}-b_2^{n-1},\ \cdots,\ w_{j+1}=b_1^{n-1}w_j^n-b_2^{n^{j+1}-1}$$

특별히 $n=2$ 이면

$$w_0=-1,\ w_1=b_1-b_2,\ w_2=(b_1-b_2)^2b_1-b_2^3,\ w_3=((b_1-b_2)^2b_1-b_2^3)^2b_1-b_2^7,\ \cdots,$$

이다. 한편 함수 $f(x)$를 사용하여

$$w_j=f_j(-b_1/b_2)\,b_2^{n^j}/b_1 \qquad (j\geq 0)$$

로 표현된다. 만약 $R=\mathbb{Z}$(정수환)이라면 단원 u는 ± 1이므로 방정식 (2)는

$$\pm\left(d^{n-1}w_{m-1}^{n/p}\right)^p\pm b_2^{n^{m-1}}=z^p$$

형태로 된다. 이 관계식은 디오판토스방정식

$$x^s + y^t = z^r \quad (s,t,r > 1)$$

에서, $s = p$, $t = n^{m-1}$ 그리고 $r = p$ 일 때 서로소인 근을 유도한다.

$$\left(\pm d^{n-1} w_{m-1}^{n/p},\ \pm b_2\ ,\ z\right)$$

$K = \mathbb{Q}$(유리수체)일 때, 다항식 $f(x) = x^n - b$은 $\mathbb{Q}$에서 기약이지만 f의 적당한 반복이 가약이 되는 원소 $0 \neq b \in \mathbb{Q}$ 들의 집합을 $S(n)$ 이라 하자. 실제로

$$S(n) = \bigcup_{m=1}^{\infty} S(n,m)$$

로 표시되며 이 때 $S(n,m)$은 다음과 같다.

$$S(n,m) = \left\{b \in \mathbb{Q}^* \mid f(x) = x^n - b,\ \mathbb{Q}\text{위에서} f_m \text{은 기약이며 } f_{m+1} \text{은 가약},\ m \geq 1\right\}$$

만약 $S(n) = \varnothing$ 이면 $f(x) = x^n - b$의 모든 반복이 기약이므로 $f(x)$의 갈로아 군을 결정할 수 있다 ([11],[13]). 한편 $S(n) \neq \varnothing$ 이면 어떤 디오판토스방정식이 자명하지 않는 근을 가지므로 디오판토스방정식 풀이에 관한 정보를 유도할 수 있다. 실제로 집합 $S(n,m)$에 대해 다음과 같은 결과가 발표되었다.

정리: [2] 위와 동일한 기호를 사용하여,

(1) $S(2,1)$ 은 무한집합이며, 따라서 $S(2)$도 무한집합이다.

(2) $S(3,m)$은 항상 유한집합이다. $m \leq 11$이거나 m이 짝수이면 $S(3,m) = \varnothing$ 이다.

(3) $n \geq 5$ 인 홀수일 때 $S(n)$은 유한이다. 특별히 $3 \nmid n$일 때 $S(n) = \varnothing$ 이다.

(4) $n = 4$ 일 때, $S(n,1) = \varnothing$ 이며 $S(n,m)$ $(m \geq 2)$ 은 유한집합이다.

(5) $n \geq 6$ 인 짝수일 때 모든 m에 대해 $S(n,m)$은 유한이다.

(6) $n > 3$ 인 짝수일 때, abc추측을 가정하면 $S(n)$은 유한집합이다. 특별히 m이 충분히 큰 값일 때 $S(n,m) = \varnothing$ 이다.

(6)에서 $S(n)$의 크기를 결정하기위해 abc추측이 사용되었으며, 이것은 결국 디오판토스방정식의 구체적인 근을 찾아내는 성과로 이어진다. 또한 abc추측과 컴퓨터 메이플 프로그램을 사용하여 위 정리에서 다루지 못한 $S(n)$들을 연구할 수 있다.

[1]에서는 abc추측을 가정하여, $m = 13$이고 $k = 1$인 경우를 제외한 모든 m과 k에 대해 $S(3^k,m) = \varnothing$를 증명하였다. 또한 $(k,m) = (1,13)$인 경우 $S(3^{13},1)$이 거의 공집합일거라는 배경을 연구하였다. $S(2,1)$는 특별한 성질을 갖고 있어서, 대부분의 집합 $S(n,m)$이 유한이거나 공집합인데 비해 $S(2,1)$는 무한집합이다. 이는 $f(x) = x^2 - b$는 기약이지만 f_2는 가약이 되는 b가 무한히 많다는 것이다. 그러나 임의의 $k > 1$이며 $m = 1$일 때 $S(2^k,1) = \varnothing$ 임을 보였다.

참고 문헌

1. Choi, E., Composition of binomial polynomial, Comm. KMS 22, 2007. 183-194.
2. Danielson, L., Fein, B., On the irreducibility of the iterates of $x^n - b$, Proc. AMS 130, 2001. 1589-1596.
3. Darmon, H., Granville, A., On Equations $z^m = F(x,y)$& $Ax^p + By^q = Cz^r$, Bull. London Math. Soc. 27, 1995. 513-543.
4. Dokchitser, T., LLL & ABC, J. Number Theory 107, 2004. 161-167.
5. Granville, A., Tucker, T., It's as easy as abc, AMS Notice 49, 2002. 1224-1231.
6. Kraus, A., On the equation $x^p + y^q = z^r$, Ramanujan J. 3, 1999. 315-333.
7. Mason, R.C., Diophantine Equations over Functions Fields. London Math. Soc., Lecture Note Ser. 96, Cambridge University Press, Cambridge. 1984.
8. Masser, D.W., On abc and discriminants, Proc. AMS 130, 2002. 3141-3150.
9. Mauldin, R.D., A Generalization of Fermat's Last Theorem: The Beal conjecture and Prize Problem, AMS Notice, 44 (11) 1997. 1436-1437.
10. Oesterle, J., New approaches to Fermat's last theorem, Semin Bourbaki, 40 (1) no. 694, Asterisque 161/162. 1987/1988.
11. Odoni, R.W.K., Realizing wreath products of cyclic groups as Galois groups, Mathematika 35, 1988. 101-13.
12. Peterson, I., The amazing abc conjecture, MAA Online. 1997.
13. Stoll, M., Galois groups over $\mathbb{Q}$ of some iterated polynomials, Arch. Math. 59, 1992. 239-244.
14. Stewart, C.L., Tijdeman, R., On the Oesterle-Masser conjecture, Monatsh Math. 102, 1986. 251-257.
15. Stewart, C.L., Yu, K., On the abc conjecture, Duke Math. J. 108, 2001. 161-181.

The Korean Journal for History of Mathematics Vol. 21 No. 3 (Aug. 2008), 113 - 126

ABC conjecture and iteration of polynomials

Department of Mathematics, Hannam University **Eun Mi Choi**

This work is devoted to study about the abc conjecture: how it works in the development of the proof of Fermat's last theorem and more generally in the diophantine equation theory. And it is also studied the application of the abc conjecture to the iteration of polynomials.

Key words: ABC conjecture, Diophantine equation, Polynomial iteration

2000 Mathematics Subject Classification: 01-02, 11D04

ZDM Subject Classification: H35

접수일 : 2008년 2월 12일 수정일 : 2008년 6월 10일 게재확정일 : 2008년 6월 15일