韓國數學敎育學會誌 시리즈 E
<數學敎育 論文集>
제 15집, 2003. 1. 189-194.

J. Korea Soc. Math. Ed. Ser. E:
Communications of Mathematical Education
Vol. 15, Jan. 2003. 189-194.

확률론적 논증을 통한 정당화 지도에 관한 연구

이 경 희 (한국교원대학교 대학원)

급격하게 변하고 있는 이 사회에 맞춰 수학이 변하고 있다. 이에 따라 학교 수학에서의 증명지도가 변해야할 필요성이 있다. 본 연구에서는 기존의 증명 개념을 아우르는 보다 포괄적인 개념으로써 정당화를 소개하고 정당화 지도 방안을 제안한다. 또, 기존의 형식적이고 엄밀한 연역적 증명과 정당화가 어떻게 다른지 비교해 보고 실제 수업하는데 도움을 줄 수 있도록 활용 방안을 간단하게 제시하고자 한다.

Ⅰ. 서 론

중·고등학교의 교육과정에서 증명은 유클리드 기하에서와 같은 전통적인 것들이고, 많은 학생들에게 증명 수업은 교사의 시범, 학생들의 모방, 암기의 패턴으로 피상적으로 이루어지고 있는 실정이다. 그 결과 학생들은 증명에 필요한 수학적인 생각을 하기 보다는 교사가 제시하는 증명 절차를 따르게 된다. 이렇듯 증명 교육의 실패원인은 절대주의 수리 철학의 영향을 받아 유클리드 기하를 중심으로 연역적이고 형식적이며 엄밀한 증명만을 강조해 온 데서 찾을 수 있다(조완영·권성룡, 2001).

또, 절대 진리로 믿어 왔던 유클리드의 공리를 의심함으로써 비유클리드가 발전하고 괴델이 공리체계에서 그 자신도 그 부정도 증명할 수 없는 명제가 그 체계 내에 반드시 존재한다는 불완전성의 정리를 증명했다. 증명의 관점이 변화하고 있는 이 시점에서 학생들에게 엄밀한 형식적 증명뿐만 아니라 정당화를 제시한다는 것은 의미가 있다.

한편, 현대는 정보화 시대로써 인터넷을 기본으로 정보처리 및 교환이 활발하게 이루어지고 있는데 여기서 정보는 개인, 기업체, 더 나아가 국가에도 중요한 자산으로 여겨지고 있기 때문에 정보보호에 관심이 높아지고 있다. 이런 정보보호를 위해 암호학에서도 소수가 결정적인 역할을 한다. 어떤 수가 소수인지 아닌지 판정하는데는 결정론적인 알고리즘에도 한계가 있다. 따라서 소수가 될 확률이 ½이면 이런 판정을 n번 반복해서 $(½)^n$의 확률이 되고 이제 소수가 아닐 확률은 $1-(½)^n$이 되는 확률론적 알고리즘을 이용한다. 이렇듯 확률을 이용한 방법이 유용하게 쓰이는 것이다(Lee & shin, 2001).

끝으로 실생활에서 다양한 형태의 정당화는 요구되어진다. 내 의견을 논리적으로 다른 사람에게 말하는 것부터 형식적이고 연역적으로는 증명하기 어려운 정리들이 정당화되어지고 있는 실정이므로 학교 수학에서 학생들에게 정당화를 지도할 필요가 있다.

따라서 본 연구에서는 다양한 정당화를 비교해 보고 수학에서 말하는 엄밀한 증명뿐만 아니라 다

른 형태의 증명을 접하게 함으로써 확산적 사고를 할 수 있도록 정당화 지도를 위한 활용방안을 간단하게 제시할 것이다.

Ⅱ. 본 론

1. 증명과 정당화

고전적인 수학적 증명은 몇 개의 공리로부터 시작한다. 공리란 사실이라고 가정할 수 있는 또는 그 자체로 사실임이 분명한 수학적 명제를 말한다. 이런 공리에서 시작하여 단계별로 논리를 전개해 나가면서 아무런 무리 없이 결론에 도달해서 하나의 수학적 증명이 완성된다. 또, 증명은 수학에서 다루는 내용의 절대적 진리성을 정당화하기 위한 유일한 방법으로써, 수학적 명제가 참임을 보증하는 이성에 근거한 핵심적인 방법으로 기능 하는 것으로 간주되었다(나귀수, 1998). 즉 증명은 절대적 진리로 인정되는 공리와 이미 참이라고 논증된 정리를 연역함으로써 정리가 참임을 보이는 수단이다.

이에 반해 정당화는 엄밀한 수학적 증명에서의 좁은 의미가 아니라 아주 간단하게 다른 사람을 설득시키는 것에서부터 임의성을 활용하는 논증기법인 확률론적 증명을 중심으로 시뮬레이션 등 다양한 논증 기법을 포함하여 상대방을 충분히 확신시키거나 설득시키기 위해서 증거가 되는 사실을 제공하는 논증 방법을 통칭한다. 즉 작은 경험으로부터 옳다고 주장하는 것, 이것을 기초 삼아 다른 특수한 경우를 테스트하는 것, 작은 것에서 일반화시키는 행위, 사고 실험 등은 정당화에 포함된다.

2. 정당화의 예

가. 영지식 증명(신현용, 1997)

한 사람이 다른 사람에게 사실의 증명에 관한 어떤 정보를 주지 않고 상대방에게 정보를 알고 있음을 증명하는 방법이다. 증명이 완료되었을 때 확인자는 증명자의 주장을 믿게 되지만 증명자가 가진 정보에 대해서는 유의미한 정보는 하나도 얻지 못하게 된다. 이 영지식 증명은 기존의 증명과는 다르게 대화형이며, 컴퓨터의 막강한 계산력이 전제되지만, 역시 임의성과 확률의 특징이 가장 결정적인 역할을 하게 된다.

나. 4색 정리(Courant R. & Robbins H., 1996; Simon, 1997)

지도에서 경계선의 일부를 공유한 이웃하는 두 나라에는 각기 서로 다른 색으로 칠하는 것이 보통이다. 이 과정에서 아무리 여러 나라가 있더라도, 또 어떻게 위치해 있더라도 서로 다른 4가지 색만을 이용하여 색칠할 수 있다는 사실이 경험적으로 알려져 있다. 이 정리의 증명은 기존의 증명과는 달랐다. 무한히 많은 모든 지도들이 4색으로 칠해질 수 있음을 증명하려면 1,482가지의 유한한 지도들만 고려하면 된다는 정리로 단순화시키고 컴퓨터로 1,482가지의 지도를 4색 문제의 조건에 맞게 칠하려면 네 종류의 색상만으로 가능하다는 결론을 얻을 수 있었다. 이것은 컴퓨터의 계산만으로 얻

어낸 최초의 수학적 증명이고, 여기서 컴퓨터는 이 문제를 해결할 수 있는 유일한 수단이었다.

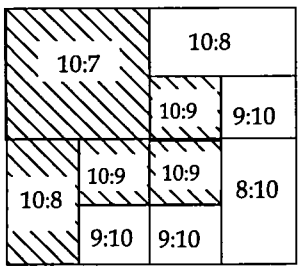
다. Monte - Carlo Method

Monet - Carlo Method는 방정식을 푸는 방식이 아니라 컴퓨터시뮬레이션 방식으로 확률을 계산하는 것을 말한다. 일반적으로 난수를 이용하여 수학의 문제를 푸는 방법을 총칭한다. 해석적으로 풀기 어려운 문제를 풀 때 자주 이용된다. 현대 암호학에서 자주 사용되는 기법이다. 이 예는 금이 그어져 있는 바닥에 바늘을 던졌을 때 바늘이 한 금과 가로질러 떨어질 확률을 구하는 뷔퐁의 바늘문제에 잘 나타나 있다.

라. 가위바위보 게임

A, B 두 사람이 가위바위보를 하고 있다. 10번을 먼저 이긴 사람에게 상금을 주기로 했는데 안타깝게도 A가 8번 이기고 B가 7번 이긴 다음에 게임이 끝났다. 상금을 어떻게 분배해야 할까?

이 문제에 대한 풀이는 확률을 이용한다. 우선 다시 한번 가위바위보를 한다면 A가 이길 확률이 ½이고 B가 이길 확률도 마찬가지고 ½이다. 이와 같은 방법으로 A든 B든 10번 이기면 게임을 마친다면 다음과 같이 그림으로 나타낼 수 있다.



<그림 1. 가위바위보 게임>

따라서, A는 상금의 $\frac{11}{16}$을 받고, B는 상금의 $\frac{5}{16}$를 가지면 된다.

마. 소수 판정법

어떤 수가 소수인지 아닌지를 판정하는 방법은 결정론적 알고리즘과 확률론적 알고리즘을 구분할 수 있다. 결정론적 알고리즘은 임의의 변수를 사용하여 소수라는 결론을 얻음으로써 100% 소수임을 판정하는 방법이고 임의의 변수를 사용하지 못하고 특정한 값들을 사용하여 소수를 판정하는 방법으로 100% 소수로 판정하지는 못하더라도 적당한 확률 이상으로 소수임을 판정하는 확률적 알고리즘이 있다.

1) 결정론적 알고리즘(김응태 · 박승안, 2002)

· 페르마의 판정법

페르마의 소정리 'p가 소수이면 p와 서로 소인 임의의 a에 대하여 $a^{(p-1)}$을 p로 나누었을 때 나머지가 1이다'를 이용하여 소수를 판정하는 방법이다. 이 정리의 역이 성립하지 않기 때문에 정리의 대우를 이용해서 소수가 아님을 증명할 수 있다. 즉 123이 소수이면 123과 서로 소인 2에 대해 2^{122}은 123으로 나누었을 때 나머지가 1이 되어야 한다. 그러나 실제로 2^{122}은 123으로 나누면 8이 된다. 따라서 123은 소수가 아니다. 더 쉽게는 123=3×41로 인수분해가 된다.

이외에도 에라토스테네스의 체에 의한 판정법, 윌슨의 판정법, 루카스의 판정법 등이 있는데 김응태 · 박승안(2002)의 정수론에 자세하게 나와 있다.

2) 확률론적 알고리즘(이민섭, 2001)

앞에서 언급한 결정론적 알고리즘은 아주 작은 소수에 대해서 소수인지 아닌지를 판정하는데도 복잡한 계산을 요구할 수 있기 때문에 현실적으로 불가능하다.

확률론적 알고리즘으로 합성수를 판정한 것은 항상 사실이지만 소수로 판정된 결론은 항상 참이 아니다. 즉 임의로 선택한 수에 대하여 여러 단계를 통과하면 적어도 확률 ½을 가지고 소수라고 할 수 있는 Solovay - Strassen 알고리즘, Lehmann - Peralta 알고리즘 등이 있고, 어떤 수 n이 k개 선택된 정수에 대하여 소수임이 판정되면, 실제로 n이 소수일 확률이 적어도 $1-(1/4)^k$이 되는 Miller - Rabin 알고리즘 등이 있다. 따라서 임의로 선택된 수가 소수로 판정되는 횟수에 따라 소수일 확률이 높아지게 되는 것이다.

정당화는 이 외에도 몬티 홀 딜레마, 아벨과 카인의 동전 던지기(최은주, 2002)등 많은 예를 들 수 있다.

이와 같이 여러 가지 정당화를 알아보았는데 기존의 증명 방법과는 다른 방법으로 문제의 해를 구하거나 확률을 이용해서 정리를 정당화를 하고 있다. 특히 컴퓨터를 이용한 4색 정리의 증명과 몬티 홀 딜레마는 직관과는 다르게 문을 옮기는 것이 더 좋다는 결론을 시뮬레이션을 통해 내리고 있고, 결정론적으로 소수를 판정하지 못하는 수를 확률론적으로 소수를 판정하는 것도 기존의 연역적인 증명과는 확연히 다르다.

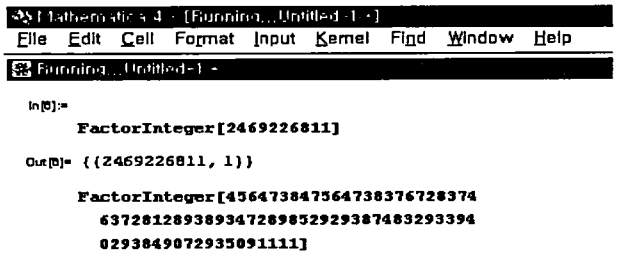
3. 활용방안

다음은 일반 고등학교에서 실제로 수업에 활용할 수 있는 예를 간단하게 제시하겠다.

◎소수 판정법

· 소수의 정의에 의해 판정하는 방법인 소인수 분해에 대해서 알아본다.

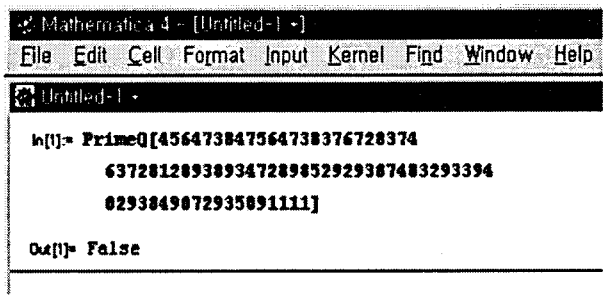
-수가 커지면 소인수 분해하는 것이 쉽지 않다는 것을 Mathematica를 통해 인식시킨다.



<그림2. Mathematica를 이용한 소인수 분해>

· 결정론적 소수 판정법
- 에라토스테네스의 체에 의한 소수 판정법, 페르마의 판정법, 윌슨의 판정법에 대해 알아본다.
- 아주 작은 소수를 판정하는데도 어려움이 따른다는 것을 인식시킨다.

· 확률론적 소수 판정법
- Mathematica를 이용해서 소수를 판정한다.



<그림3. Mathematica를 이용한 소수 판정법>

- 앞에서 했던 소인수 분해와 소수 판정하는 것이 동일한 문제가 아님을 인식시킨다.

Ⅲ. 결 론

본 연구에서 제시한 정당화는 실생활에 연결된 수학을 가르침으로 해서 수학에 대한 거부감을 감소시키고 흥미를 유발시켜 학습하는데 긍정적인 태도를 기를 수 있다. 또, 실험과 관찰, 컴퓨터 시뮬레이션 등을 통해서 교실에서 시간적이나 공간적인 이유로 실제 할 수 없었던 상황을 실제와 유사한 상황으로 제시함으로써 학생들로 하여금 실제 상황으로 한 걸음 다가가게 할 수 있다.

마지막으로 학습 분위기를 토론과 활동 등을 할 수 있는 열린 분위기로 만들어서 학생들의 확산적인 사고와 적극적이고 능동적인 학습 태도의 유도로 인해 학생들끼리 의사 소통하고 교사와의 상호작용에 의해 자신의 생각을 반성함으로써 문제를 하나하나 풀어 나가면서 경험할 수 있는 장점이

있다.

유클리드 기하학을 통한 엄밀한 수학적 증명은 수학에서 가장 소중하고 아름다운 부분이고 꼭 배워야 하는 부분이다. 사회 환경은 물론, 수학, 학생들의 자세나 취향이 급격히 변하고, 기존의 증명 지도에 여러 가지 문제가 야기됨으로 학교 수학에서의 증명 지도에 근본적인 변화를 시도할 때라고 생각한다(신현용, 2002). 이 글에서는 여러 상황을 고려하여 볼 때, 보다 넓은 의미에서의 증명, 즉 정당화를 지도하여 학생들로 하여금 현 실생활에 더욱 효과적으로 적응할 수 있을 것이다. 이는 동시에 현재의 수학적 증명이 정당화와 차별화 되어 특징인 엄밀성의 가치와 아름다움이 오히려 돋보이고 보존될 수 있을 것이다.

본 연구에서는 정당화를 고찰하고 활용방안을 잠시 언급했는데 보다 확실히 하고, 발전시키기 위해 다음과 같이 제언하고자 한다.

첫째, 본 연구를 토대로 확률론적 논증 이외에도 다양한 정당화의 교수·학습 자료가 개발되어야 한다. 학생들에게 탐구할 수 있는 가운데 수학적 개념을 획득할 수 있는 자료를 발굴하여 체계적인 학습자료로서의 개발이 이루어져야 한다.

둘째, 본 연구에서 개발한 자료를 학생들을 대상으로 투입하여 효과를 검증하지 않았다. 이에 대한 후속 연구가 필요하다.

참 고 문 헌

김응태·박승안 (2002). 정수론(4판). 서울: 경문사.

나귀수 (1998). 증명의 본질과 지도 실제의 분석 - 중학교 기하 단원을 중심으로, 서울대학교 박사학위논문.

신현용 (1997). 영지식 증명, 한국수학교육학회 뉴스레터 **13(4)**, pp.23-25.

_____(2002). 학교수학에서의 증명지도의 재조명, 한국수학교육학회지지 시리즈 E <수학교육 논문집>, **14**

이민섭 (2001). 현대암호학. 서울: 교우사.

조완영·권성룡 (2001). 학교수학에서의 '증명', 대학수학교육학회지 수학교육연구, **11(2)**, pp.385-402.

최은주 (2002). 인지갈등을 통한 학습자료개발과 적용, 한국교원대학교 석사학위논문.

Courant, R. & Robbins, H. (1996). What is Mathematics?(2nd ed.). London: Oxford University Press, Inc. 박평우, 김운규, 정관택(역) (2002). 수학이란 무엇인가, 서울: 경문사.

Lee, K. & Shin, H. (2001). Proofs for gifted students. *Journal of Korea Society of Education Series F: Studies in Mathematical Education* **6**, pp.167-177.

Simon S. (1997). Fermat's last theorem. London: Christopher Little Literary Agency. 박병철(역) (2002). 페르마의 마지막 정리. 서울: (주)영림카디널.