Commun. Korean Math. Soc. **19** (2004), No. 4, pp. 585–599

초청논문

학교수학에서의 정당화 지도의 필요성 및 가능성에 관한 연구

신현용

ABSTRACT. 본 연구에서는 학교수학에서 증명지도의 문제점을 정당화의 측면에서 분석하고, 정당화의 한 방법으로서 확률론적 정당화를 제시하며, 학교수학에서 정당화 지도의 교육적 가치, 정당화 지도의 방향, 정당화 지도의 예와 지도 방법에 대해 논의한다. 이러한 논의에 근거하여 학교수학에서의 정당화 지도의 필요성 및 가능성에 관하여 살펴본다. 본 연구에서 '증명'은 고전적인 의미에서의 증명, 즉 엄밀한(rigorous) 증명, 수학적(mathematical) 증명이고, '정당화'는 기존의 수학적 증명 개념은 물론, 다양한 논증 기법을 포함하는 넓은 의미이다.

1. 시작하는 말

제 7차 수학과 교육과정 [1] 에서 수학 교과는 '수학의 기본적인 개념, 원리, 법칙을 이해하고, 사물의 현상을 수학적으로 관찰하여 해석하는 능력을 기르며, 실생활의 여러 가지 문제를 논리적으로 사고하고 합리적으로 해결하는 능력과 태도를 기르는 교과'로서 성격이 규정되어 있다. 그런데 논리적으로 사고하고 합리적으로 해결한다는 것은 전통적으로, 가정(assumptions)이나 주어진 사실로부터의 논리적 추론을 통해 결론을 유도하는 것을 의미해 왔다. 이러한 논증에서는 주어진 조건들, 공리로서 참임이 인정된 명제들, 그리고 이미 증명된 명제들을 이용하여 어떤 명제가 참임을 유도해야 했다. 유클리드 원론의 '증명(proof)'은 이러한 추론의 전형적인 예라고 할 수 있다. 유클리드 원론은 정의, 공리, 공준, 이미 참임이 증명된 명제들을 바탕으로 엄밀한 논리적 추론을 통해 새로운 명제를 순차적으로 증명하는 모범을 보여주고 있다. 그 결과, 얼마 전까지만 해도 수학에서 증명이란 유클리드 원론에 제시된 타당성 입증의 틀을 의미하는 것으로 받아들여져 왔다. 그런데, 근래에 수

Received June 11, 2004.
2000 Mathematics Subject Classification: 97B70, 97D20.
Key words and phrases: 학교수학, 증명, 정당화, 확률론적 논증.
본 연구는 한국교원대학교 2003 기성회계 지원에 의하여 수행되었다.
본 연구 과정에서 경상대학교 한인기 교수의 도움이 컸다.

리철학 분야에서 증명의 본질에 대한 다른 해석이 제기되었고 [30], 순수 수학 분야에서도 몇몇 새로운 논증 기법들을 활용하여 명제의 타당성을 입증하였다. 사색문제(four color problem) [43]나 공 쌓기 문제(Kepler's conjecture) [40]의 해결은 새로운 논증 기법 활용의 대표적인 예라고 할 수 있다. 이러한 문제의 해결 과정에서는 유클리드 원론에 제시된 틀, 즉 전통적인 수학적 증명과는 다른 접근을 취하고 있다. 이러한 변화는 증명 뿐만 아니라 수학 자체에 관해서도 활발한 논의를 유발하였다 [15, 16, 26, 27, 30]. 분명한 사실은 수학의 본질에 대한 인식이 급격히 변하고 있다는 것이다. 사회가 변하고 수학이 변하면 수학교육도 필연적으로 변해야 하는데, 수학교육이 변하는데 소요되는 시간은 수학이 변하는데 소요되는 시간보다 훨씬 길 수밖에 없고, 또 길어야 한다. 수학 교사 양성과 재교육(연수)이 선행되고, 학교 수학 교육과정이 변하는 데에 그 만큼 상당한 기간이 필요하기 때문이다. 따라서 수학교육자는 급격한 수학의 변화를 주시하고, 이에 따른 수학교육의 변화에 대해 신중하게 숙고해야 한다. 최근 우리나라 수학교육계의 증명에 관한 많은 관심 [2, 3]은 주목할 만 하다.

한편, 정보사회에서 정보의 보호와 정보의 효율적인 통신은 중요한 문제인데, 이에 관련된 학문 분야로 암호학(cryptography)과 부호이론(coding theory) 등을 생각할 수 있다. 이들 분야에서는 다양한 정당화 기법을 개발하여 실생활에 이미 활용하고 있다는 사실도 수학교육자는 주목할 필요가 있다. 학교수학의 내용과 관련하여서도, 피타고라스 정리나 삼각형 세 내각의 합에 관한 정리는 종이를 오려 붙이거나 GSP 등을 활용하여 설득력 있게 정당화할 수 있다. 또는, 컴퓨터에 의한 실험이나 관찰만으로도 주장하는 바의 정당성을 충분히 확보할 수도 있을 것이다. 이와 같이 주어진 명제의 타당성을 보이는 방법은 여러 가지가 있을 수 있다. 본 연구에서는, 이러한 논증 기법 모두를, 고전적인 증명의 일반 개념으로서 정당화(verification, justification)라고 부른다. 교육적 측면에서의 정당화에 관한 연구로는 신현용 [8], 박주희 [6], 신송임 [7] 등이 있다. 이들 연구에서는 다양한 정당화 기법들을 소개했다는 측면에서는 의미가 있지만, 수학교육에서 정당화의 도입 필요성 및 효과적인 활용에 관한 체계적인 연구는 수행되지 못했다. 본 연구에서는 학교수학에서 증명지도의 문제점을 정당화의 측면에서 분석하고, 정당화의 한 방법으로 확률론적 정당화를 제시하며, 학교수학에서 정당화 지도의 교육적 가치, 정당화 지도의 방향, 정당화 지도의 예와 지도 방법에 대해 논의한다. 이러한 논의에 근거하여 학교수학에서의 정당화 지도의 필요성 및 가능성에 관하여 살펴본다. 이 연구를 통해, 학교수학에서 전통적인 증명을 포괄하는 개념인 정당화에 대한 체계적인 연구의 기초를 제공하고, 학생들이 합리적으로 사고하고 문제를 해결할 수 있는 수학교육의 방향을 제시할 수 있을 것이다.

2. 확률론적 정당화

확률(임의성)은 수학적으로 다루기 용이하지 않은 속성을 가지고 있다 [21]. 그러나, 임의성은 논증에서 강력한 힘을 발휘할 수 있음이 알려지면서, 수학의 여러 분야에서 확률의 다양한 활용 방법이 연구되고 있다. 그 중에서 주목할 만한 것으로, 정보 보호 기능을 가지는 유익한 논증이 가능하다는 것이다. 먼저 확률의 까다로운 속성을 간략히 고찰하고, 확률을 활용한 논증 방법인 확률론적(probabilistic) 정당화를 살펴보자.

가. 확률의 난해성

확률의 신비한 속성은 확률이론의 발달 과정에서도 쉽게 알 수 있다. 다음은 확률의 속성이 수학의 가장 기본적인 문제를 야기함을 말해준다: Although randomness can be precisely defined and can even be measured, a given number cannot be proved to be random. This enigma establishes a limit to what is possible in mathematics [21]. 수학의 다양한 역설 중 상당수가 확률과 관련된다 [34]는 사실에서도 확률 개념의 난해함을 짐작할 수 있다. 유명한 예 중 하나는 '두 봉투 역설(two-envelope paradox)'인데, 그 내용은 다음과 같다: 당신 앞에 상금이 들어 있는 두 봉투가 놓여 있다. 한 봉투 안에 있는 상금의 액수는 다른 봉투에 들어 있는 상금의 액수의 두 배이다. 이제 당신은 봉투 하나를 택하여 그 안의 상금 액을 확인한다. 그 후 언제라도 당신은 당신의 선택을 한번은 바꿀 수 있다. 당신이라면 바꾸겠는가? 이미 택하여 확인한 봉투의 상금이 x원이라고 하자. 다른 봉투 속의 상금이 $2x$ 원일 확률과 $x/2$원일 확률은 똑같이 1/2이다. 따라서 당신의 선택을 바꿨을 경우, 상금의 기대값은 $x + x/4$ 원이다. 즉, 현재 확보한 상금인 x원보다 많다. 따라서 당신은 당신의 선택을 바꿔야 한다. 위의 논증과 그 논증의 결과는 타당한가? 타당하지 않다면 무엇이 문제인가? 사실, 이 질문에 대한 답은 자명하지 않은 것 같다. Chalmers [22] 등을 참고하면 좀 더 깊이 있는 분석을 볼 수 있다. 또 하나의 유명한 예는 소위 Monty-Hall dilemma라고 불리는 것인데, 이에 대해서는 여러 곳 (예를 들어, Hoffman [25])에 소개되었으므로 여기서는 재론하지 않기로 한다. 확률의 난해성을 알 수 있는 더 많은 예는 Paulos [34], 이충호 [11], Kapadia 와 Borovcnik [28] 등에서 볼 수 있다.

나. 확률의 힘

위에서 언급한 바와 같이 확률(임의성)은 상당히 난해한 속성을 가지고 있다. 그러나 확률은 한편으로는 강력한 논증을 가능하게 하기도 한다. 폴 에어디쉬가 그래프 이론에 임의성을 도입하여 소개한 Random Graph Theory는 이러한 접근의 하나라고 할 수 있다. 울람(S. Ulam)과 폰 노이만 등이 세계 제2차 대전 중에 수행된 핵무기 개발 프로젝트에

참여하여 확률론적 방법으로 여러 난제를 해결했음은 주지의 사실이다. 바바이는 여러 가지 가정과 이론을 임의성의 가정 하나로 대치될 수 있음을 보이고, 그 기능을 활용하여 강력한 논증 체계를 소개하였다 [17]. 한편, 골드바서 등 [24]과 브라사 등 [19]은 '영지식 증명(zero-knowledge proof)'이라고 불리는 정보 보호에 유용하고 효과적인 논증 기법을 소개하였다. 영지식 증명에는 기존의 증명과는 다르게 대화형(interactive)이며, 컴퓨터의 막강한 계산력이 전제되지만, 역시 확률의 속성이 가장 결정적인 역할을 하게 된다. 그러나, 이렇게 다양한 형태의 논증 방법이 소개되는 과정에서 '어떤 방법은 "증명(proof)"이고 어떤 방법은 증명이 아닌 단순한 "논증(argument)"이다'라고 하는 것과 같은 증명 개념에 많은 혼란이 초래되었다. 이러한 혼란은 최근 수학에서 소개되는 또 다른 형태의 논증 방법들과 어울리면서, 문제가 더욱 더 복잡해졌다. 본 연구에서는 이러한 논증 기법 모두를 통칭하여 '정당화'라고 부르고 있다. 위에서 언급한 '영지식 증명'은 이 글의 용어로는 '영지식 정당화'다.

다. 확률론적 정당화의 예

(1) 암호학에서 어떤 자연수 a 가 소수인가를 판정하는 것은 매우 중요하다. 전통적인 관점에서는 a 의 소인수를 찾아 a 가 소수인가 합성수인가를 판정할 것이다. 그런데, 현대의 암호학에서는 a 를 소인수분해하지 않고, a 가 소수 또는 합성수임을 선언한다. 컴퓨터에 의한 이 주장은 사실 확률론적 선언이다. 좀더 정확하게 말하면 '주어진 수가 소수(또는 합성수)일 확률은 거의 1 이다'와 같은 선언이다. 결국 전통적인 수학에서는 소수판정은 소인수분해와 분리될 수 없는, 근본적으로 동일한 문제이지만, 컴퓨터를 활용한 현재의 방법에서는 두 문제는 다른 문제라는 것을 알 수 있다. 사실, 소인수분해(factoring)는 현실적으로 계산이 불가능한(infeasible, untractable) 문제이지만, 소수판정(primality test)은 현실적으로 계산이 가능한(feasible, tractable) 문제다. 부록에 제시된 실험결과(MATHEMATICA 활용)는 이러한 사실을 보여준다. 그 예를 통하여 소인수분해에는 상당한 시간을 요구하지만 소수판정에는 그렇지 않음을 알 수 있기 때문이다. 사실, 100자리의 두 소수의 곱인 합성수를 소인수분해하는 것은 아직까지 소개된 최고의 프로그램과 최고 성능의 컴퓨터를 이용해도 현실적으로 가능하지 않다. 양자계산(quantum computing)과 양자컴퓨터(quantum computer)는 이러한 관점에서 주목할 만 하다. 양자계산 기법과 양자컴퓨터가 실용화되면 소인수분해 등과 같은 계산복잡성의 문제가 대부분 해결될 것이기 때문이다. 최근 소수 판정의 다항함수 시간(polynomial time)의 결정론적 알고리즘이 소개되었다. 자세한 내용에 대해서는 Agrawal, Kayal와 Saxena [14] 또는 Bornemann [18]을 참조할 수 있다.

(2) 앞에서 언급한 골드바서 등 또는 브라사 등에 의하여 제안된 영지식 정당화도 대표적인 확률론적 정당화 기법이다.

(3) 명자(증명자)가 가지고 있는 주머니 안에 바둑돌 2개가 들어있다. 직접 만져보면 이 사실을 쉽게 확인할 수 있다. 이제, 명자는 주머니를 열어 그 내용물을 보여주지 않고 그 안에 있는 두 개의 돌이 모두 흰색임을 정당화하려 한다. 먼저 명자는 인자(확인자)에게 주머니 속을 들여다보지 말고 돌 하나를 꺼내서 그 색을 확인하도록 한다. 명자의 주장이 사실이라면, 그 돌은 흰 색이다. 이때, 명자가 거짓말을 할(주머니 속에 검은 돌이 들어있을) 확률은 1/3 이다. 이제 그 돌을 주머니 속에 다시 넣고 흔들어(임의화하고, randomize), 인자에게 전과 같은 요령을 반복하도록 한다. 이 과정을 20 번 반복한다. 명자의 주장이 사실이라면, 각 단계에서 뽑는 돌은 모두 흰색일 것이다. 그런데 인자의 입장에서는 명자가 거짓말을 할(주머니 속에 검은 돌이 들어있을) 가능성도 있다고 생각하는데, 그 확률은 $(1/3)^{20}$ 이 되어 거의 0 이다. 이 상황에서 인자는 명자의 주장을 옳은 것으로 받아들일 것이다. 이 프로토콜에서 인자가 원한다면 실험 횟수를 얼마든지 늘릴 수 있다. 이 정당화는 영지식 증명은 아니다. 왜냐 하면, 정당화 과정에서 '주머니 안에 흰 돌이 적어도 하나는 있다'는 의미 있는 정보를 노출하였기 때문이다.

(4) 대수적부호이론 (Algebraic Coding Theory)에서의 복호 (decoding) 기법인 최근방 복호법 (nearest neighborhood decoding)의 이론적 기초에는 확률이 있다. 한 예를 들어보자 [12]. 최소거리 (minimum distance)가 5 인 이진(binary) 선형부호(linear code) $\{00000, 11111\}$ 는 두 비트까지의 오류(error)를 수정할 수 있다. 수신벡터가 00001 일 때, 이는 000C0 로 복호된다. 이는 00000 이 00001 로 전송될 확률이 11111 가 00001 로 전송될 확률보다 크기 때문이다. 마찬가지로 수신벡터가 01101 일 때, 이는 11111 로 복호된다. 이는 11111 이 01101 로 전송될 확률이 00000 이 01101 로 전송될 확률보다 크기 때문이다. 결국, 부호이론에서 복호원리의 정당성도 확률론적으로 확보됨을 알 수 있다.

라. 확률 개념의 수학교육적 활용

확률의 유용하면서도 편리한 이러한 속성은 학교 수학에서의 정당화 지도에 유용하게 활용될 수 있다. 확률 활용의 예를 이해하는 데에는 확률의 기초적인 개념과 성질 외에는 어려운 확률 이론이 필요하지 않은 것도, 학교수학에서 확률론적 정당화 지도를 용이하게 하는 이유가 될 것이다. 실제로, 확률의 기본 속성을 활용하는 몬테칼로 기법(Monte Carlo method)은 학교 교실에서 활발히 적용되고 있다. 이 방법의 기본 원리는 간단하여 중등학교 수준에서도 성공적으로 지도될 수 있기 때문이다. 예를 들어, Brunner [20]는 몬테칼로 기법을 활용하여 협동 학습 모형을 제시하였고, Geer [23]도 몬테칼로 기법이 실생활에서 얼마나 유용한가를 예를 통하여 설명하였다. 한편, McClintock 과 Jiang [32]에 의한 Excel Spreadsheets 활용 학습도 몬테칼로 기법에 의한 것이다.

3. 수학교육에서의 현행 '증명' 지도의 문제점(정당화의 측면에서)

수학에서의 증명의 중요성은 재론할 필요가 없다. 그러므로, 수학교육에서의 증명 지도는 그 필요성과 중요성이 확실하다. 그러나 기존의 증명 지도에는 여러 문제점이 있음을 지적할 수 있다.

먼저, 현행 제7차 수학과 교육과정 8-나(중학교 2학년 2학기)에서 본격적으로 가르치고 있는 증명 단원에 대해서 대부분의 보통 학생이 특히 어려워한다. 교육 현장에서는 이 문제를 해결하고자 많은 노력을 하고 있으며, 그 중 하나가 증명 지도에 컴퓨터를 도입하여 그 어려움을 만회하고자 하는 것이다. 그러나 이러한 접근은 자칫 증명 교육의 본질에서 벗어나게 되고, 증명 지도는 고사하고, 학생들로 하여금 증명 개념에 심각한 혼란을 초래하게 하는 등 여러 부작용이 야기시킬 수도 있을 것이다. 또한, 8-나 수준의 보통 학생들은 증명하고자 하는 주장에 대하여 엄밀한 수학적 증명의 필요성을 느끼지 않는 경우도 많다. 종이 오리기나 붙이기 또는 컴퓨터 등에 의한 직관적인 정당화의 수준을, 교과서가 요구하는 엄밀한 수학적 증명의 논리적 수준과 구별하지 못하는 경우도 많다. 설령, 이러한 수준의 차이를 이해하여 수학적 증명의 가치를 인정한다 하더라도, 그 엄밀한 논증 체계를 소화하기가 용이하지 않다. 따라서 엄밀한 수학적 증명 지도는 보다 뒤의 단계에서 이루어지도록 하는 것을 고려해볼 만하다. 게다가 증명에 관한 현행 교과서의 접근에 여러 가지 문제점이 지적되기도 하였다 [13]. 많은 학생들이 증명 단원에서 수학에 대하여 흥미를 잃거나, 심지어 수학을 싫어하게 된다는 현장 교사들의 증언도 귀 기울일 필요가 있다.

둘째, 실생활에서는 엄밀한 논증 못지 않게 정당화 수준의 논증이 자주 사용된다. 엄밀한 증명 능력은 학생들의 체계적이고 논리적인 사고력을 향상시킬 것이다. 그러나 실생활에서는 수학적 증명 수준의 논증보다 정당화 수준의 논증이 더 자주 활용되는 경우가 많다. 학교 수학이 실생활과 밀접히 연관될 필요가 있다는 점에서 정당화 수준의 논증 능력 함양에도 중점을 둘 필요가 있다. 게다가 학교 수학은 고도의 수학적 능력을 함양시켜 유능한 수학자나 과학자를 양성하는 것이 주목적은 아닐 것이다. 또한, 컴퓨터 등을 쉽게 활용할 수 있는 환경에서는 강력한 정당화가 매우 용이하다는 점도 주목할 가치가 있다. 이렇게 볼 때, 학교 수학에서 엄밀한 수학적 증명에 초점을 맞추고 정당화를 간과하는 것은 재고될 필요가 있을 것이다.

셋째, 괴델의 불완전성정리(Gödel's incompleteness theorem) [33] 이후 고전적인 수학적 증명은 그 절대 권위를 상실하였다고 볼 수 있다. 따라서 여러 가지 현실적인 어려움에도 불구하고 그러한 논증만의 교육을 고집하는 것은 문제가 있다고 할 수 있다. 더구나 논리 정연한 체계보다 직관적인 체계가 더 가치를 부여받을 수 있는 경우가 자주 있다. 수학은 그 당시의 시대적, 문화적 흐름과 무관할 수 없다는 것을 고려

하면, 전통적인 수학 체계만을 고집하는 것이 바람직하다고는 할 수 없을 것이다.

이 외에도 여러 가지 문제점을 생각할 수 있겠으나, 위에서 기술한 이유만으로도 학교 수학에서 현재의 증명 지도는 재고되어야 하고, 더 나아가 새롭게 제시되어야 한다는 주장을 제기할 수 있을 것이다. 다만, 2000년 이상 전해 내려온 전통적인 '증명'의 의미와 가치는 지속적으로 존중되어야 하고, 어느 것도 '증명'이라는 수학의 근간을 훼손하여서는 안 될 것이다. 따라서 기존의 증명 지도 내용은 크게 변화시키지 않으며, 다만 증명을 정당화의 특수한 개념으로 지도함이 바람직하다고 할 수 있겠다.

4. 정당화 지도의 방향

정당화 지도의 필요성과 가능성에 관해서 더 많은 논의와 합의가 이루어져야 하겠지만, 정당화 지도가 학교 수학에서 이루어진다고 할 때, 정당화의 지도 방향을 앞선 논의에 근거하여 다음과 같이 제시할 수 있을 것이다.

가. 현행 교육과정에서는 본격적인 증명 지도가 8-나 수준에서 아무런 사전의 예비 과정 없이 이루어진다. 엄밀한 증명 기법을 익히기가 쉽지 않다는 점을 감안하면 이와 같은 갑작스런 증명 지도는 학생들로 하여금 큰 어려움을 야기시킬 것이다. 따라서 정당화 지도는 초등학교부터 점진적으로 지도되어야 할 필요가 있다.

나. 다양한 실험과 관찰, 컴퓨터 시뮬레이션 등을 통하여 여러 가지 정당화 기법에 익숙하게 하고, 그러한 정당화 기법이 실생활에 유용함을 알게 한다.

다. 실생활의 여러 예를 통하여 정당화(설득) 과정의 필요성을 알게 한다. 이 과정은 초등학교부터 시도할 필요가 있으며, 충분히 가능할 것이다. 초등학교에서는 증명 또는 정당화와 같은 자연스럽지 못한 개념의 사용이나 의식화 없이, 생활 가운데 경험할 수 있는 대화를 통하여 그러한 환경을 설정하고 매우 초보적인 수준의 정당화 기법을 익히도록 한다.

라. 중학교 수준에서는 엄밀한 증명은 자제한다. 대신 종이 오리기와 붙이기, 종이 접기, 컴퓨터 등에 의한 실험과 관찰을 토대로 다양한 정당화를 지도한다. '삼각형에서 세 내각의 합에 관한 정리'나 '피타고라스 정리'는 위와 같은 접근이 매우 용이하다. 이 때, 상식적이거나 직관적인 논증이 오류를 발생시킬 수 있음을 경험하게 하여 엄밀한 논증의 필요성을 깨닫고, 그러한 논증을 시도하게 한다. 그러나 이 때에도 엄격한 '증명'은 피하고, 다양한 실험이나 관찰, 컴퓨터 시뮬레이션에 의한 방법 등 학생들이 흥미를 가지며, 충분한 설득력을 확보할 수 있는 정당화를 지도하도록 한다.

마. 고등학교 수준(10 단계 이후)에서 본격적인 수학적 증명을 다룬다. 이 단계의 학생들은 앞 단계에서 배운, 관찰이나 실험에 근거한 결과나 주장은 완벽한 타당성을 보장하지 못함을 인식할 것이다. 따라서 전통적인 수학적 증명에서 최종적인 타당성은 결코 관찰이나 실험에 의존하지 아니함을 주지시킨다. 이 단계에서는 유클리드 기하학이나 기본적인 정수론 등을 통하여 엄밀한 수학적 증명을 지도한다. 이 단계에서도 수학적 증명에만 국한하지 않고, 컴퓨터 시뮬레이션 등을 통한 정당화의 지도와 적절한 확률론적 정당화의 지도도 학생들의 수준에 따라 지도하는 것이 바람직하다. 여기서 말하는 확률론적 정당화의 경우는, 중학교 단계에서 다룬 정당화보다 그 타당성이 더 확보됨을 설득력 있게 설명할 수 있다. 이 때 분명히 하여야 할 것은 정당화 방안 지도의 핵심은 유클리드 기하학에서의 고전적 증명이라는 것이다. 이 증명이야말로 수학에서 결코 소홀히 되어서는 안 되고 [41, 42], 다른 논증 기법과 혼동되어서도 안 된다.

바. 주어진 문제에 대하여 다양한 정당화 방안을 제시할 수 있도록 지도하는 것은 바람직하다. 한 예로 Monty Hall dilemma의 에 대하여 다음과 같이 세 가지 정당화를 제시할 수 있다.

(1) Hoffman [25]에 소개된 것처럼 경우의 수를 따져본다.

(2) 신현용·최은주 [10]에 소개된 것처럼 Excel Spreadsheets을 사용하여 정당화한다.

(3) Bayes 정리를 적용하여 확률을 직접 계산한다.

사. 정당화 지도 과정에서 학생들로 하여금 적절한 글이나 교양도서를 추천하여 읽게 하는 것은 매우 효과적일 것이다. 몇 가지 좋은 소재를 들면 다음과 같다: Hempel's paradox [36], Banach-Tarski 역설 [9], Pólya [35], 박병철 [4], Hoffman [25].

아. 과학고등학교나 영재학교에서는 물론 일반적으로 호기심이 많은 학생에게는 암호학은 좋은 소재가 될 수 있다 [31, 39]. 약간의 계산적인 사실을 설명해주면 영지식 증명, RSA 공개열쇠 암호체계, 전화로 동전 던지기(coin flipping by telephone), 열쇠 분배(key distribution), 전자 서명(digital signature) 등의 기법도 설명이 가능하다 [39]. 이러한 내용을 가르치고자 할 때에, 교사는 박승안 [5]과 Kranakis [29]등을 참고할 수 있다. 다음 두 실험 [38]은 컴퓨터 활용을 좋아하는 학생에게 유익할 것이다.

(1) 학생들로 하여금, 소인수 분해 문제는 컴퓨터를 사용하더라도 만만치 않은 문제임을 경험시키기 위하여 다음 실험을 하도록 한다. 소인수 분해 문제의 이러한 특징은 현대 암호학에서 매우 중요한 역할을 하므로, 이 실험은 의미가 크다고 할 수 있다. 이 실험에서 학생들은 소인수 분해(factoring)와 소수 판정(primality test)은 근본적으로 같은 문제로 인식할 것을 전제한다.

(가) 먼저 BASIC이나 LOGO를 사용하여 다음 두 프로그램을 짜도록 한다. 학생들이 프로그램 짜는 것을 부담스러워하면 교사가 제공해도 된다. 또는 http://primenumber.pe.ky/ 에 접속하여 Primenum.exe를 사용하도록 한다.

· 주어진 자연수를 소인수 분해한다: 이 때 학생들은 기본적인 알고리듬을 사용할 것을 전제한다.

· 주어진 자연수를 이진법으로 표현한다.

(나) 다음 형태의 수에 대하여 이진법 프로그램을 구동하고 그 결과를 관찰하라: $2^k-1, 1 \leq k \leq 10$. 이 수들은 k 개의 1 로 이루어짐(repunit number)을 발견할 것이다. 이는 이진법의 원리로부터 금방 알 수 있는 사실임을 설명한다.

(다) 위 (나)의 결과를 참고하여 , 임의의 자연수 k 에 대하여 2^k-1 형태의 수가 소수일 필요조건을 찾아라. 1 의 개수를 나타내는 k 가 합성수이면, 원래의 수도 합성수임을 쉽게 알 수 있다. 따라서 k 가 소수여야 함은 하나의 필요조건이 된다. 이제 이 필요조건은 충분조건인가를 몇 가지 실험을 통하여 조사하고 싶다.

(라) 다음 수들에 대하여 소수 판정하여라: 2^3-1, 2^5-1, 2^7-1, $2^{11}-1$.

이 실험의 결과, k 가 소수인 것은 주어진 수가 소수이기 위한 충분조건이 아님을 알게 된다. 그러면 '소수 k 가 어떤 수일 때 주어진 수가 소수일까'라는 질문이 가능하다. 이 실험에서는 이 질문에 대한 해답을 찾지 않는다. 단지 소인수분해가 컴퓨터를 사용하여도 간단한 문제가 아님을 알게 하고자 한다. 이를 위하여 k 를 크게 하여 프로그램을 구동시킨다. 그러나 계산에 많은 시간이 소요된다. 즉, k 가 조금만 더 커져도 계산은 쉽게 끝나지 않음을 관찰하게 될 것이다. 이 실험을 통하여 소인수의 문제가 계산상 간단한 일이 아님을 경험하게 된다.

(마) 이제 고급 프로그램을 활용하여 보자. MAPLE이나 MATHEMATICA 등을 활용하여 두 수, $2^{19}-1, 2^{23}-1$ 에 대하여 소수인가를 판정하여라. 필요한 프로그램의 코딩이 여의치 못한 경우에는 http://primenumber.pe.ky/에서 프로그램 코드를 볼 수 있다. 위의 소프트웨어에 대한 접근 자체가 용이하지 않을 때에는 http://primenumber.pe.ky/에 접속하여 타원곡선을 이용한 소인수분해 프로그램을 활용하면 된다. 학생들의 프로그램보다 훨씬 효율적임을 알 수 있다. 그러나 k 가 너무 커지면 (극단적인 예를 들면, $k = 4423$), MATHEMATICA도 실행하지 못함을 관찰한다. 이 단계에서 소인수분해의 계산상의 특징을 설명하여 준다. 또, MATHEMATICA의 구동 원리와 우리 프로그램의 구동 원리의 차이를 알고리듬 측면에서 설명한다. 이 글의 부록은 이에 관한 설득력 있는 실험 결과이다.

(바) 다음 웹 사이트를 방문하여 최근 발견된, 큰 메르센(Mersenne) 소수에 대하여 알아보아라: http://www.mersenne.org/primes.htm. 큰 소수의 발견에 관한 여러 가지 흥미로운 사실도 알게 될 것이다.

(2) 컴퓨터 계산상으로는 소수 판정의 문제와 소인수 분해의 문제는 완전히 다른 문제임을 다음 실험을 통하여 경험하게 한다. 이 글 부록의 실험 결과는 이 프로젝트의 결과이다.

(가) MATHEMATICA이나 MAPLE 등을 활용하여 $k = 5, 10, 15, 20, 25, 30$ 인 경우 다음 계산을 한다: 자리수가 k 개인 두 소수를 임의로 생성하라.

(나) 아주 쉽게 계산을 수행한다는 사실을 알 수 있다. 이 정도 크기의 수에 대하여 소수 판정이 용이하다는 것임을 알게 한다.

(다) 위에서 생성한 두 수를 곱하여 그 합성수를 n 이라고 놓아라.

(라) 얻은 수 n 에 대하여 소수 판정하여라. 소수 판정과는 상황이 다름을 알 수 있다. 어떤 수의 경우는 합성수임을 알면서 그 수의 소인수는 하나도 모르는 경우도 가능하다는 것이다. 이 단계에서 확률론적 기법의 힘(유용성)을 설명한다. 소수 판정은 $10, 20, ..., 50$ 자리의 수는 물론 이보다 매우 큰 경우에도 쉽게 수행한다는 사실을 알 수 있다.

(마) 얻은 수 n 을 소인수 분해하여라.

(바) 위의 실험 결과에 대해서 다각도로 논의하여 보자. 예를 들어 다음과 같은 설명이 가능할 것이다. 위의 실험 결과를 모두 제시함으로써 다음 주장을 정당화할 수 있다: 위에서 사용한 프로그램(MAPLE 이나 MATHEMATICA)에서는 입력된 수에 대한 소수 판정은 소인수분해에 의하지 않는다.

5. 맺는 말

이 글에서 학교수학에서 증명지도의 문제점을 정당화의 측면에서 분석하고, 정당화의 한 방법으로 확률론적 정당화를 제시하며, 학교수학에서 정당화 지도의 교육적 가치, 정당화 지도의 방향, 정당화 지도의 예와 지도 방법에 대해 논의하였다. 또, 이러한 논의에 근거하여 학교수학에서의 정당화 지도의 필요성 및 가능성에 관하여 살펴보았다. 이 글에서 '증명'은 고전적인 의미에서의 증명, 즉 엄밀한 증명, 수학적 증명이고, '정당화'는 기존의 수학적 증명 개념은 물론, 다양한 논증 기법을 포함하는 넓은 의미로 사용되었다. 수학 분야에서 활용되는 정당화의 대표적인 예를 확률론적 정당화에서 찾아볼 수 있다. 암호학에서 어떤 수가 합성수임을 판정하는 것은 실제로 나누어 떨어짐의 확인을 통한 방법에 의한 것이 아니라, '주어진 수가 소수(또는 합성수)일 확률은 거의 1 이다'와 같이 확률적이다. 현대의 암호학에서 널리 활용되는 영지식 증명도 확률론적 정당화의 한 방법이다. 이처럼 확률론적 정당화의 방법은 강력한 적용가능성으로 인하여 현대 수학의 다양한 분야에

폭넓게 활용되고 있다. 정당화와 관련하여, 현행 수학교육에서 발생되는 엄밀한 증명 지도의 문제점으로, 첫째 직관적인 수준에서 수학적 심상이 형성되지 못하고 엄밀한 증명의 필요성을 인식하지 못한 상태에서 중학교 2학년 학생들에게 엄밀한 증명을 요구하기 때문에, 수학에 대한 흥미를 잃게 되는 경우가 많다. 둘째, 실생활에서는 엄밀한 논증보다는 정당화가 폭넓게 활용되기 때문에, 엄밀한 논증만을 강요하는 것은 '실생활과 연계된 수학교육'이라는 시대적 요구에 부응하지 못한다. 셋째, 괴델의 불완전성 정리 이후 고전적인 수학적 증명은 절대 권위를 상실하였으며, 수학 분야에서 이미 다양한 정당화 기법이 사용되고 있기 때문에, 교육현장에서 엄밀한 증명지도만을 고집하는 것은 수학사적인 흐름을 거스르는 것이라 할 수 있다. 본 연구에서는 정당화 지도의 방향으로 첫째, 갑작스런 엄밀한 증명 지도는 학생들로 하여금 큰 어려움을 야기시키기 때문에, 초등학교부터 점진적으로 정당화 지도가 이루어져야 하며, 둘째 다양한 실험과 관찰, 컴퓨터 시뮬레이션 등을 통하여 여러 가지 정당화 기법에 익숙하게 하고, 그러한 정당화 기법이 실생활에 유용함을 알게 해야 한다. 셋째, 실생활의 여러 예를 통하여 정당화(설득) 과정의 필요성 및 기초적인 정당화 기법을 알게 하며, 넷째 중학교 수준에서는 엄밀한 증명은 자제하며, 종이 오리기와 붙이기, 종이 접기, 컴퓨터 등에 의한 실험과 관찰을 토대로 다양한 정당화 방안을 지도한다. 다섯째, 고등학교 수준(10 단계 이후)에서 본격적인 수학적 증명을 다룬다. 여섯째, 주어진 문제에 대하여 다양한 정당화 방안을 제시할 수 있도록 지도하는 것이 바람직하다. 본 연구의 결과는 학교수학에서 전통적인 증명을 포괄하는 개념인 정당화에 대한 체계적인 연구의 기초를 제공하고, 학생들이 합리적으로 사고하고 문제를 해결할 수 있는 수학교육의 의미있는 방향을 제시할 것으로 기대된다.

References

[1] 교육부, *제 7차 수학과 교육과정*, 서울: 대한교과서주식회사, 1997.

[2] 대한수학교육학회, *증명지도*, 제 38회 수학교육학 집중세미나 자료집, 2002.

[3] 대한수학교육학회, *The Nature of Proof*, 제 43회 수학교육학 집중세미나 자료집, 2004.

[4] 박병철 역, *페르마의 마지막 정리*, 영림카디널, 1999.

[5] 박승안, *대수학과 암호학*, 경문사, 1999.

[6] 박주희, *점진적 구성의 증명지도를 위한 학습자료 개발 연구*, 한국교원대학교 석사학위논문, 2000.

[7] 신송임, *비형식적 정당화를 활용한 증명지도 사례 연구*, 한국교원대학교 석사학위논문, 2004.

[8] 신현용, *영지식증명. 한국수학교육학회 뉴스레터 제 13권 제 4호*, 서울 : 한국수학교육학회(1997), 23–25.

[9] 신현용·승영조 역, *무한의 신비*, 승산, 2002.

[10] 신현용·최은주, *인지갈등에 의한 수학 영재교육*, 수학교육학술지: 한국수학교육학회시리즈 F, 제5집, 서울:한국수학교육학회(2000), 155–163.

[11] 이충호 역, *이야기 파라독스*, 사계절, 1990.
[12] 조영수·강주호, *선형형대수학 제2판* , 경문사, 2004.
[13] 한인기·강인주, *삼각형 무게 중심의 증명에 관한 다양한 접근 방법들*, 수학교육논문집: 한국수학교육학회시리즈 E, 제10집, 서울: 한국수학교육학회 (2000), 143–154.
[14] M. Agrawal, N. Kayal and N. Saxena, *PRIMES is in P*, IIT Kanpur preprint; http://www.cse.iitk.ac.in/news/primality.html (2002).
[15] G. E. Andrews, *The death of proof? Semi-rigorous mathematics? You've got to be kidding!*, The Math. Intelligencer **16** (1994), no. 4., 16–18.
[16] M. Atiyah et al., *Responses to theoretical mathematics: Toward a cultural synthesis of mathematics and theoretical physics*, Bull. Amer. Math. Soc. **30** (1994), no. 2, 178–211.
[17] L. Babai, *Trading group theory for randomness*, Proc. 17th Annual ACM Symposium on the Theory of Computing (1985), 421–429.
[18] F. Bornemann, *PRIMES is in P: a breakthrough for "Everyman"*, Notices Amer. Math. Soc. **50** (2003), no. 5, 545–552.
[19] G. Brassard, D. Chaum and C. Crépeau, *Minimum disclosure proofs of knowledge*, J. Comput. System Sci. **37** (1988), no. 2, 156–289.
[20] R. Brunner, *The telephone directory and probability*, Mathematics Teacher, December (1997).
[21] G. J. Chaitin, *Randomness and mathematical proof*, Scientific American, May (1975), 47–52.
[22] D. J. Chalmers, *The Two-Envelope Paradox: A Complete Analysis?*, http:// www.u.arizona.edu/ chalmers/papers/envelope.html (2001).
[23] C. Geer, *Factoring uncertainty into retirement planning: The Monte Carlo Method*, Fortune, January (1999).
[24] S. Goldwasser, S. Micali and C. Rackoff, *The knowledge complexity of interactive proof system*, Proc. 17th Annual ACM Symposium on the Theory of Computing (1985), 291–304.
[25] P. Hoffman, *The Man Who Loved Only Numbers*, Hyperion, New York(1998): 신현용 역. 우리 수학자 모두는 약간 미친 겁니다, 승산, 1999.
[26] J. Horgan, *The death of proof*, The Scientific American **269** (1993), 92–103.
[27] A. Jaffe and F. Quinn, *Theoretical mathematics: Toward a cultural synthesis of mathematics and theoretical physics*, Bull. Amer. Math. Soc. **29** (1993), no. 2, 1–13.
[28] R. Kapadia and M. Borovcnik (Eds.), *Chance encounters: probability in education*, Kluwer Academic Publishers, 1991.
[29] E. Kranakis, *Primality and Cryptography*, B. G. Teubner (1986).
[30] I. Lakatos, *Proofs and Refutations*, New York: Cambridge University Press, 1976.
[31] K. S. Lee and H. Shin, *Proofs for Gifted Students*, J. Korea Soc. Math. Educ. Ser. F: Studies in Mathematical Education **6** (2001), 167–177.
[32] E. McClintock and Z. Jiang, *Spreadsheets: Powerful tools for probability simulations*, Mathematics Teacher, October (1997).
[33] E. Nagel and R. Newman, *Gödel's Proof*, New York University Press, 1958.
[34] J. A. Paulos, *Innumeracy*, Penguin Books, 1988.
[35] G. Pólya, *How to solve it*, New York: Doubleday, 1957.
[36] W. C. Salmon, *Confirmation*, Scientific American **269** (1973), 75–83.

[37] H. Shin, *A Brief Survey of Zero-Knowledge Proofs*, J. Korea Institute of Information Security and Cryptology 4 (1994), no. 2, 39–54.
[38] ———, *A mathematical program for high schools of gifted students*, In preparation.
[39] H. Shin and I. Han, *Mathematics Education for Gifted Students in Korea*, A Regular Talk. ICME9, Tokyo, Japan (2000).
[40] G. G. Szpiro, *Kepler's Conjecture*, Wiley, 2003.
[41] R. Thom, *"Modern"Mathematics: An Educational and Philosophic Error?*, The American Scientist **59** (1971), no. 6, 695–699.
[42] ———, *Modern mathematics: does it exist?*, in Howson(Ed.), Development in Mathematical Education (1973), 194–209.
[43] R. Wilson, *Four Colors Suffice*, Princeton, 2002.

부록

다음 실험에서는 먼저 실험 목적에 맞는 크기 (15 에서 19 자리까지)의 소수 두 개를 임의로 생성하게 한다. 그 후 그 두 소수를 곱하여 한 합성수를 얻는다. 그리고 그 합성수가 소수인지 합성수인지 검사하게 하고 그 때 소요되는 시간을 기록하게 한다. 마지막으로 그 합성수를 소인수분해하게 하고 그 때 소요되는 시간을 기록하게 한다. 다음 자료는 그 실험 결과의 일부이다. 이 자료로부터 MATHEMATICA이나 MAPLE 등에서 사용하는 소수 판정 알고리즘과 소인수분해 알고리즘의 근본적인 차이를 알 수 있다.

Generating two 15 digit prime numbers:
x : 434629305430289, y : 665467547741617
Multiplying these two numbers:
x*y : 289231698061336681936377637313
Is this a prime number? False
time for testing primality = 0.00,
time for factoring = 12.16

Repeating the same process for 16 through 19 digit numbers:
x : 8631210886513459, y : 4733291607536417
x*y : 40854038052011113227349503136403
Is this a prime number? False
time for testing primality = 0.00,
time for factoring = 29.73

x : 43844943313217821, y : 60419894818445839
x*y : 2649106863305340959624973298096819
Is this a prime number? False
time for testing primality = 0.00,
time for factoring = 28.01

x : 636726278910913649, y : 774368972868523853
x*y : 493061074598641443022958194179769597
Is this a prime number? False
time for testing primality = 0.00,
time for factoring = 111.70

x : 6018091022426304037, y : 8614712799432196969
x*y : 518441257590438781208680291936638638 53
Is this a prime number? False
time for testing primality = 0.00,

time for factoring = 223.48

한국교원대학교 수학교육과
충북 청원군 강내면 다락리
363-791
E-mail: shin@knue.ac.kr