A DIALOGIC METHOD OF PRESENTING PROOFS: FOCUS ON FERMAT'S LITTLE THEOREM

Boris Koichu* and Rina Zazkis**

* Technion – Israel Institute of Technology
** Simon Fraser University

Twelve participants were asked to decode a proof of Fermat's Little Theorem and present it in a form of a script for a dialogue between two characters of their choice. Our analysis of these scripts focuses on issues that the participants identified as 'problematic' in the proof and on how these issues were addressed. Affordances and limitations of this dialogic method of presenting proofs are exposed, by means of analyzing how the students' correct, partial or incorrect understanding of the elements of the proof are reflected in the dialogues. The difficulties identified by the participants are discussed in relation to past research on undergraduate students' difficulties in proving and in understanding number theory concepts.

Key words: proof as dialogue; students' difficulties with proving; number theory; equivalence by modulus; Fermat's Little Theorem

Introduction

The extensive professional literature on mathematical proof and proving tells us that virtually any aspect of understanding and producing mathematical proofs is a stumbling block for learners (cf. Knapp, 2005, Harel & Sowder, 2007, for comprehensive reviews). As a rule, students' difficulties with constructing and understanding proofs are exposed by means of documenting and interpreting their (often poor) performance when coping with various proving tasks. This research approach implies that students' understanding of proofs and their difficulties are mainly examined from an expert point of view. A complementary approach – inquiring what students themselves see as issues of difficulty – is still underrepresented in research on proof and proving. As such, the goals of our study were to inquire what students themselves perceive as problematic issues in a given non-trivial proof in number theory, to compare these with the expert view, and to describe how students cope with the identified difficulties.

Theoretical underpinnings

Our study is influenced by the idea of writing a fictional script of interaction as a part of a learning process. In particular, we refer to the dialogical approach for presenting proofs (Gholamazad, 2006, 2007), and to a "lesson play" (Zazkis, Liljedahl, & Sinclair, 2009; Zazkis, Sinclair, & Liljedahl, 2013). The roots of these methods are inspired by the style of Lakatos's (1976) evocative *Proofs and Refutations* and can be traced to a Socratic dialogue, a genre of prose in which a 'wise man' leads a discussion, often pointing to flaws in thinking of his interlocutor.

Gholamazad (2006, 2007) introduced the dialogical method of presenting proofs in her work with prospective elementary school teachers. This type of proof presentation consists of a script of a dialogue between characters that ask and answer questions about different steps in a proof. Gholamazad suggested that the dialogical method provided insights into the students' cognitive obstacles when creating and interpreting proofs. She developed the method based on Sfard's (2001, 2008) communicational framework, which conceptualizes thinking as a form of communication, specifically, as "individualized version of *interpersonal communication*" (Sfard, 2008, p. 81, italics in the original). The idea was that a request for a student to present a proof in a form of a dialogue makes his or her personal thinking salient. As such, in assigning the Task for our participants (see Figure 2) we expected to learn about their explanations of concepts and justifications of claims presented in the given proof that may not be apparent in a 'standard' form of presenting a proof.

Further, the idea of learning-via-scripting was implemented in teacher education in a different context, referred to as a "lesson play" (Zazkis, Liljedahl, & Sinclair, 2009; Zazkis, Sinclair, & Liljedahl, 2013). A lesson play is a novel construct in research and teachers' professional development in mathematics education. Using the theatrical meaning of the word 'play', lesson play refers to a lesson or part of a lesson written by a teacher or a prospective teacher in a script form, featuring imagined interactions between a teacher and her students. In teacher education, it provided a valuable tool for engaging prospective teachers in considering particular students' mistakes or difficulties, presented in prompts that serve as a starting point for the play. In research, it provided a window on how prospective teachers envision addressing students' difficulties, both mathematically and pedagogically. In particular, the prospective teachers' personal understanding of the mathematics involved became apparent in their attempts to guide students' solutions. As such, we wondered what mathematical understandings would surface when students decode proofs through script-writing.

Our Study

In light of the above considerations, our study addresses two interrelated research questions:

(1) What problematic issues do students identify in the given proof and how do they deal with these issues when decoding the proof into a script? In particular, which issues are treated as central?

(2)What can be learned from the dialogue method of presenting a proof about participants' understanding of particular concepts in number theory that appear in the given proof? In particular, how are students' correct, partial or incorrect understandings of the number theory concepts reflected in their scripts?

Twelve students participated in our study. Two of them were graduate students in mathematics education; the other 10 were working towards completion of a teaching certificate for secondary mathematics. At the time of the study the participants were enrolled in an elective course entitled "Proofs and proving", taught by the second author. An extensive mathematical background – an undergraduate degree in mathematics or in mathematics education – is required for teaching certification at the location of the study. Therefore, all the participants had broad exposure to undergraduate mathematics, having completed at least eight upper-division courses, including a course in Number Theory.

<u>Theorem:</u> For prime number p and natural number a, such that $(a, p) = 1$, $a^{p} \equiv a \ (mod\ p)$
<u>Proof:</u> $0, 1, 2, \ldots (p-1)$ is a list of all possible remainders in division by p.

When these numbers are multiplied by a, we get $0, a, 2a, 3a, \ldots (p-1)a$. When the numbers are reduced by p we get rearrangement of the original list.

Therefore, if we multiply together the numbers in each list (omit zero), the results must be congruent modulo p: $a \times 2a \times 3a \times \ldots \times (p\text{-}1)a \ \equiv \ 1 \times 2 \times 3 \times \ldots \times (p\text{-}1) \ \ (mod\ p)$

Collecting together the a terms yields $a^{p-1}(p\text{-}1)! \equiv (p\text{-}1)! \ (mod\ p)$

Dividing both sides of this equation by $(p-1)!$ we get

$a^{p-1} \equiv 1 \ (mod\ p)$ or $a^{p} \equiv a \ (mod\ p)$, QED.

Figure 1: Fermat's Little Theorem and its proof (adapted from Wikipedia)

The participants responded to the Task related to a theorem and its proof presented in Figure 1. Based on the mathematical background of the participants, we expected that they were familiar with all the concepts and symbols presented in the proof. The fact that the theorem is Fermat's Little Theorem was not announced, but we assumed that at least some of the students would recognize it from their prior studies. The Task is presented in Figure 2.

Create a dialogue that introduces and explains the attached theorem [see Figure 1] and its proof. Highlight the problematic points in the proof with questions and answers. In your submission:

- Describe the characters in your dialogue.
- Write a paragraph on what you believe is a "problematic point" (or several points) in the understanding of the theorem/statement or its proof for a learner.
- Write a dialogue that shows how you address this hypothetical problem (THIS IS THE MAIN PART OF THE TASK)
- Add a commentary to several lines in the dialogue that you created, explaining your choices of questions and answers, in connection to the characters, which may not be obvious for the reader.

Figure 2: The Task

Results and Analysis

In the initial stage of analysis we examined, first independently and then together, each student's work for problematic issues, which were explicitly identified as such in the students' comments or dealt with in the script. We considered a problematic issue to be "dealt with in the script" if there was an excerpt, in which the dialogue's characters explicitly addressed the issue with questions and answers. Further, a problematic issue was considered to be a 'central problematic issue' if it was explicitly identified by a participant as such, or if its discussion took significantly more space than discussions of the other issues. At the second stage of the analysis two kinds of problematic issues, for which the data seemed to have provided rich and solid evidence, were isolated: (1) gaps in the flow of the proof, and (2) the presumed lack of preliminary knowledge. The space allocation allows us only to exemplify briefly each kind.

Gaps in the flow of the proof

Focus on "rearrangement of the remainders". The proof in Figure 1 is not explicit about the reasons for why reducing the numbers *0, a, 2a, 3a, …, a(p-1)* by *p* results in the rearrangement of the list of remainders *0, 1, 2, 3, …, p-1*. This point can be decoded, for instance, by assuming that there are two numbers on the list *0, a, 2a, 3a, …, a(p-1),* which give the same remainder when divided by *p*, and concluding that this assumption is wrong as it contradicts the conditions that *p* is a prime number and that *a* and *p* are co-primes.

Ten out of 12 students treated this issue as problematic, and six of the 12 treated this issue as a central one. Most students provided correct arguments based on the proof by contradiction. Only 2 mistakenly assumed that a reminder of *ka* is *k* (e,g., remainder of *3a* is *3*). To our surprise, which was informed by the literature about students' difficulties with the logic of indirect proofs (e.g., Brown, 2012; Leron, 1985; Tall, 1979; Koichu et al., 2012), most participants did not consider, at least not explicitly, the logical structure of proof by contradiction as a possible source of difficulty.

Focus on the properties of multiplication and division in equivalence relations. The "rearrangement of the remainders" step of the proof is needed in order to justify the multiplication in modular statements, that is, to justify the equivalence $a \times 2a \times 3a \times ...(p-1)a \equiv 1 \times 2 \times 3 \times ...(p-1) \pmod{p}$. Seven out of 12 students elaborated on why this congruence holds in their scripts, and 6 of them presented mathematically accurate explanations.

However, while the multiplication is easily explained based on the rearrangement of reminders, division in a congruence statement appeared to us as the second problematic point due to a gap in the proof. Why the equivalence remains when both sides of a modular congruence are divided by *(p-1)!* is not explained. Decoding this issue requires recalling the fact that dividing both sides of a congruence by a number does not always preserve the equivalence (e.g., 12 ≡ 16 (mod 2) is true, but the division of both sides by 4 – 3 ≡ 4(mod 2) – results in a false statement). In the given proof, the division is possible because it is given that *p* is a prime number, and thus $(p-1)!$ and *p* are co-primes.

For some participants the treatment of division appeared to be similar to that of multiplication, without attending to the modulus. Apparently, the inevitable analogy between operations with regular equations and operations with modular arithmetic equations is responsible for these students' confusion. The analogy is particularly salient in the following excerpt taken from one of the scripts.

Teacher: Let's divide both sides by *(p-1)!* and get $a^{p-1} \equiv 1(\text{mod } p)$.
Student: Is it allowed to divide like this?
Teacher: Yes. *p* is a prime number, so it is different from 1, therefore, *(p-1)* is different from 0 and so it is possible to divide by it.

As we see, the teacher-character argues that the division is possible just because it is not division by 0. Thus, she acts as if the same justification that applies to 'regular' algebraic and arithmetic expressions also applies in the modular case. Of the nine students that treated this issue in their scripts, four made this assumption. The (problematic) role of the analogy between familiar algebraic equations and modular equivalencies is further discussed below.

The presumed lack of preliminary knowledge

Focus on the meaning of equivalence relation. The formal mathematical definition of congruence, introduced by Gauss in his 1801 work *Disquisitiones Arithmeticae*, states the following: For *a, b* $\in N$ $c \equiv b$ *(mod m)* if and only if *m* divides |*c*-*b*| . In other words, natural numbers *c* and *b* are said to be congruent modulo *m* if they have the same remainder in division by *m*. In particular, with respect to the statement of the theorem discussed here, a^p and *a* have the same remainder in division by *p*. However, in the common usage of congruence, what appears on the right hand side of the equivalence statement is the remainder in division of the left hand side by the modulus. That is, while statements (1), (2) and (3) below are all correct according to the definition, (1) is the one that is usually used when working with congruence classes of integers.

(1) 13 ≡ 3 (*mod* 5); (2) 3 ≡ 13 (*mod* 5); (3) 13 ≡ 8 (*mod* 5)

This is likely what leads to a rather common view that the right hand side of the congruence statement indicates the remainder. Consider the following examples from two different scripts, where the first exemplifies the meaning of mod and the second defines it:

Student: I have never seen the word 'mod', what does it mean?
Teacher: Modulo means the remainder in division of whole numbers. For example, 7 modulo 6 equals 1 because the remainder in division [of 7 by 6] is 1. How much is 22 modulo 5?
Student: If we divide 22 by 5, we get 4 and remainder 2, therefore modulo it is 2.

***

Asker: What is the meaning of $a^p \equiv a(\text{mod } p)$?
Researcher: It means that when a^p is divided by *p* the remainder is *a*.

We found similar misinterpretations in 5 scripts. Actually, this claim about the remainder holds true only if *a* is smaller than *p*. For cases where *a* is larger than *p*, the remainder in division of a^p by p (or anything else by p) should be smaller than p (by the definition of a remainder), as such it cannot be a. Consider a simple example of a=3 and p=2. The remainder in division of 3^2 by 2 is 1, and not 3.

The misinterpretation of congruence relations is rather common and was noted in prior research. When the participants in Smith's (2002) study were asked in an interview to explain the meaning of the statement $a \equiv b(\bmod n)$, five out of six students gave the following interpretation: "*a* divided by *n* has a remainder of *b*." This is despite the fact that three appropriate equivalent definitions were provided by the professor teaching their course.

These responses are reminiscent of the extensive research literature on young children treating the equality sign as an instruction to find a solution, rather than an indication of equivalence (e.g., Behr, Erlwanger & Nichols; 1980, Booth, 1988; Kieran, 1981, Matthews et al., 2012). While the resemblance between the misconceptions in both cases can be explained by an inappropriate analogy, one of the dialogues offers another possible reason: the influence of programming experience. The command *mod* in Pascal, as well as in several other programming languages and mathematical programs, is a function of two variables that outputs a remainder.

Focus on the basic concepts. In some scripts we find extended attention to clarifying all the concepts that appear in the theorem. While we agree with the view that understanding of the underlying concepts is essential, we believe that at the stage of dealing with the given theorem most of the concepts should not be problematic for a learner. The following is an excerpt from one of such scripts.

Impatient: The statement says that for 2 co-prime numbers *a* and *p*, where *p* is prime and a is natural, the remainder in division of a^p by *p* is *a*.
Clueless: Wait a second, what are co-prime numbers?
Impatient: This is when their greatest common divisor is 1.
Clueless: And what is a common divisor?
Impatient: This is some whole number, which divides the two numbers and gives whole quotients.
Clueless: Can you give an example?
Impatient: Yes indeed, 3 for example is the greatest common divisor of 3 and 6.
Clueless: Why is this true?

The next 25 lines of the dialogue clarify and exemplify concepts of prime, co-prime, divisor, factorial and division with remainder. Only then the dialogue proceeds to the proof itself. Surprisingly, when all the concepts are clarified, the lines of the proof are presented with minimal explanation. However, the issues that most of the participants (as well as we) considered as problematic are simply restated without additional explanation. This corresponds to the participant's stated belief that complete understanding of all the concepts in the theorem paves the way for understanding the proof.

We noted that those students, who were less successful in the course in general, devoted in their dialogues unnecessary extended attention to details that could be considered 'trivial', or taken for granted at the expected level of mathematical sophistication. They then passed quickly through the statements that required clarification. Such extended attention to particular concepts appears to us as a 'shield' that protects the students from exposing their personal difficulties in understanding the 'real' problematic sections of the proof.

Conclusions and Contribution

Within a wide variety of research in mathematics education that attended to undergraduate students' ability to handle proofs, the tasks presented to students requested them to produce proofs (e.g., Smith, 2006) or to evaluate given proofs (e.g., Selden & Selden, 2003). The task of interpreting a given correct proof in the form of a script for a dialogue is a relatively novel approach that provides several methodological advantages.

The approach enabled us to reveal which issues the students chose to pause on and explain, how mathematical issues are treated in these explanations, and what is taken as shared understanding or assumed knowledge. A possibility to choose a focus of the dialogue and decide on time and space allocation of various issues can be considered both as an affordance and a limitation of the method. The issue of affordance is clear as the dialogue provides an opportunity of explaining what is not apparent in the dry formalism of mathematical proofs. However, it also provides an opportunity to avoid "real problematics" by directing the focus of attention to other issues.

We conclude that the task of working through a proof and presenting it in the form of a dialogue proved to be fruitful on several accounts: it provided a window into students' abilities to handle identified difficulties; it exposed misconceptions as well as personal strengths. Our contribution can be seen on several arenas: methodological innovation in task design and implementation, further insight on understanding proofs by students with strong mathematical backgrounds, and extension of research on understanding particular concepts in number theory.

References

Behr, M. J., Erlwanger, & Nichols (1980). How children view the equals sign. *Mathematics Teaching*, 92, 13-15.

Booth, L. R. (1988). Children's difficulties in beginning algebra. In A. F. Coxford (Ed.), *The Ideas of Algebra, K-12* (pp. 20-32). Reston, VA: National Council of Teachers of Mathematics.

Brown, S. (2012). Making jumps: An exploration of students' difficulties interpreting indirect proofs. *Electronic Proceedings for the 15th Annual Conference on Research in Undergraduate Mathematics Education*. Portland, OR. Retrieved March 17, 2012, from: http://sigmaa.maa.org/rume/crume2012/RUME_Home/Home.html

Gholamazad, S. (2006). Pre-service elementary school teachers' experiences with interpreting and creating proofs. *Unpublished doctoral dissertation*. Simon Fraser University.

Gholamazad, S. (2007). Pre-service elementary school teachers' experiences with the process of creating proofs. In Woo, J. H., Lew, H. C., Park, K. S. & Seo, D. Y. (Eds.), *Proceedings of the 31st Conference of the International Group for the Psychology of Mathematics Education*, Vol. 2, pp. 265-272. Seoul, Korea: PME.

Harel, G., & Sowder, L. (2007). *Toward a comprehensive perspective on proof*, in F. Lester (Ed.), *Second Handbook of Research on Mathematics Teaching and Learning* (pp. 805-842), NCTM, Reston: VA.

Kieran, C. (1981). Concepts associated with the equality symbol. *Educational Studies in Mathematics*, 12, pp. 317-326.

Knapp, J. (2005) Learning to prove in order to prove to learn. [Online]: Retrieved September 17, 2012, from http://mathpost.asu.edu/~sjgm/issues/2005_spring/SJGM_knapp.pdf

Lakatos, I. (1976). *Proofs and refutations.* Cambridge: Cambridge University Press.

Leron, U. (1985). Direct approach to indirect proofs. *Educational Studies in Mathematics*, 16(3), 321-325.

Matthews, P., Rittle-Johnson, B., McEldoon, K., & Taylor , R. (2012). Measure for measure: What combining diverse measures reveals about children's understanding of the equal sign as an indicator of mathematical equality. *Journal for Research in Mathematics Education*, *43*(3), 316-334.

Selden, A., & Selden, J. (2003). Validation of proofs considered as texts: Can undergraduates tell whether an argument proves a theorem? *Journal for Research in Mathematics Education*, 34(1), 4-36.

Sfard, A. (2001). There is more to discourse than meets the ears: learning from mathematical communication things that we have not known before. *Educational Studies in Mathematics,* 46(1-3), 13-57.

Sfard, A. (2008). *Thinking as communication: Human development, the growth of discourses, and mathematizing.* Cambridge, MA: Cambridge University Press.

Smith, J. C. (2002). Revisiting Algebra in Number Theoretic setting. In Campbell. S. R., & Zazkis, R. (Eds.) *Learning and teaching number theory: Research in cognition and instruction* (pp. 249-283). Westport, CT: Ablex.

Smith, J.C. (2006). A sense-making approach to proof: Strategies of students in traditional and problem-based number theory courses. *Journal of Mathematical Behavior*, 25(1), 73-90.

Tall, D. O. (1979). Cognitive aspects of proof, with special reference to the irrationality of $\sqrt{2}$. In *Proceedings of the 3rd Conference of the International Group for the Psychology of Mathematics Education* (pp. 203–205).Warwick.

Tall, D., Yevdokimov, O., Koichu, B., Whiteley, W., Kondratieva, M., & Cheng, Y.-H. (2012). *Cognitive development of proof*. In M. De Villiers & G. Hanna (Eds.), *Proof and proving in mathematics education* (pp. 13-49). New York, NY: Springer.

Zazkis, R., Liljedahl, P., & Sinclair, N. (2009). Lesson Plays: Planning teaching vs. teaching planning. *For the Learning of Mathematics, 29*(1), 40-47.

Zazkis, R., Sinclair, N., & Liljedahl. P. (2013, in press). *Lesson Play in Mathematics Education: A tool for research and professional development*. Springer.