

The Development of Knowledge and Claims of Truth in the Autobiography *In Code*

Sarah Flannery had the rare experience in this era of producing new mathematical research at the age of 16. When preparing her project to enter the Esat Young Scientist Exhibition in Ireland, she explained that she felt undaunted by the task of attempting to prove something new in mathematics because she had had the experience of watching her mathematician father and his physicist friend wrestle with mathematical problems before. By watching their struggles and discoveries, she realized that mathematicians do not a priori know all the answers, that there is still further mathematical knowledge to be developed, and that she need not question her ability to investigate a problem just because she has an incomplete background (Flannery, 2001). Her experiences, together with a brief history of the field of mathematics that she studied, shed light on how mathematical knowledge is developed. Specifically, they demonstrate the important role of curiosity and further questioning in generating topics of inquiry and the role of tools such as computers and the academic literature in directing/shaping that inquiry. Additionally, a contrast of her sub-area of cryptography with the wider field of number theory gives insight into what makes something true or accepted in this arena. Specifically, her story demonstrates that cryptography has standards of proof closer to the natural sciences than to its parent discipline of number theory.

Role of Curiosity and Further Questioning

Flannery's father regularly gave his children logical puzzles to stimulate their mathematical interest. Her experience with these puzzles illustrates the role of curiosity, logic, and further questioning in developing knowledge. One puzzle episode outlined in the book involved the magic square in which a 3x3 grid must be filled with the numbers 1 through 9 so

that the sum of each row, each column, and each diagonal is 15 (Flannery, 2001). She describes her process of initially guessing and checking some possible solutions, but eventually stopping to do some explicit reasoning. From this reasoning, she determines that the only possible number that can go in the middle square is 5, that the number 9 must be in a non-corner cell, and that once she chooses which side of 9 the 4 will lie on, the rest of the puzzle is completely determined. Having answered the original question, she thought she would move on, but her father declared there was more to investigate.

He asked her to determine how many 3x3 magic squares there were in all. This is an instance where further penetrating questions can produce and/or formalize greater knowledge. As a result of her methodical earlier reasoning, she could then easily prove there were exactly eight possible valid configurations. Reflecting on this experience, Flannery comments that “by exploring just a bit beyond what you were initially asked you could end up proving something” (Flannery, 2001, p. 256).

Flannery and her father give a brief tour of number theory in her autobiography to introduce the background to her work. This tour outlines some of the directions of mathematical research in number theory that have developed out of initial curiosity followed by further questioning. For example on the tour, they ask “How do you factor a number? How many prime numbers are there? Is there a formula for generating prime numbers?” (Flannery, 2001, p.50). These simple questions have actually motivated significant mathematical discovery by revealing deep properties of our number systems and motivating further penetrating questioning.

Standard of Proof in Number Theory

One product of this questioning was Euclid's proof that there are infinitely many primes. This example sheds light on the standard of proof in number theory and most mathematical

areas. Euclid's proof used the technique of *reductio ad absurdum*, or proof by contradiction. This proof technique begins by assuming that your assertion is false, then tracing through the logical consequences of that assumption to find that at some point the assumption leads to a logical contradiction. This method of following through the logical implications of an argument is the foundation of the formal proof mathematicians seek; such a proof guarantees that the result will be true now and forever, which is the standard of truth mathematicians have come to expect.

If no such proof is known, but a significant body of evidence supports a belief, then the belief may be accepted by the mathematical community as a conjecture. Even when a significant body of evidence is accumulated, though, there is no guarantee that the claim will turn out to be true. For example, in exploring the question of how to generate prime numbers, Chinese mathematicians from the 5th century BC came to believe they could characterize all prime numbers by the following statement:

$$n \text{ is prime if and only if } n \text{ is a factor of } 2^{n-1} - 1;$$

a description they developed from playing with hundreds of examples. The forwards implication of this statement is in fact true, although it was not formally proven until Fermat conquered it in 1640. The backwards implication, however, turns out to be false, even though it is true for the first 340 numbers! It was not until 1820, over two millennia later, that someone discovered that 341 is a factor of $2^{340} - 1$, but 341 is not prime since it equals 11×31 (Flannery, 2001). This extreme example demonstrates that even when something is known to be true in a large number of cases, that finite truth may not extrapolate to hold in all possible cases.

Standard of Proof in Cryptography

Such examples of the failures of finite truths have driven mathematicians to search for definitive proofs of their claims. But within the area of cryptography, this goal has been elusive

due to the nature of the problems posed, and so a different standard of proof has been accepted.

The purpose of cryptography is to transmit a message between two parties in a secure way so that anyone overhearing the message cannot uncover what the message said. To this end, a *one-way function* is often employed, which is an operation that is easy to perform, but extremely difficult, if not impossible, to undo/invert (Flannery, 2001). A non-mathematical example of such a function is the mixing of black and white paint to obtain gray – the mixing is easy, but ever recovering the black or white paint from the gray appears impossible. Although this last claim seems obvious, one cannot produce a formal proof that no method exists to recover the original paint colors. This issue of the difficulty of generating a formal proof is why the standard of proof in cryptography is so different from that in other areas of mathematics.

The primary one-way function used in cryptography is multiplication of large primes because no efficient algorithm has ever been found for factoring large numbers; this function is the basis of the prevailing public-key cryptosystem known as the RSA algorithm. The creators of this algorithm explain in their foundational paper: “since no techniques exist to prove that an encryption scheme is secure, the only test available is to see whether anyone can think of a way to break it ... once the method has withstood all attacks for a sufficient length of time it may be used with a reasonable amount of confidence” (Flannery, 2001, p.175-6).

Flannery's personal experiences in cryptography further illustrate the expectations for proof in the field. Flannery began her science project by studying the RSA algorithm, but eventually she helped to develop an alternative cryptosystem that was hypothesized to provide significant speed and security gains. After formalizing the algorithm and verifying its speed gains, she had the formidable task of establishing that her algorithm was equally secure. Flannery explains “the only way to know is to envisage all sorts of attacks and then show

(hopefully) that none can succeed ... Another person might see a gaping hole in the system, but you hope this won't happen, and if it does, you try to deal with it" (Flannery, 2001, p. 206).

This standard of proof is incredibly different from what is seen in number theory and mathematics in general. As we saw with the ancient Chinese belief about primes, evidence for a finite number of cases does not prove something will always be true. In that same vein, the ability of a cryptosystem to withstand a finite number of attacks cannot prove that it will always be secure, but within cryptography, this standard of proof seems to be the best one can hope for.

It is worth recalling a few scenes from *Fermat's Enigma* to show that this same situation of potential fallibility of proof can, in fact, crop up in other areas of mathematics. For example, Cauchy and Lamé both believed they had successfully proven Fermat's Last Theorem, but Kummer pointed out a gaping hole in the logic of their proof. Similarly, Wiles believed that he had proven Fermat's Last Theorem, but Katz identified an error that could have foiled the whole proof had Wiles not been able to patch together a new solution (Singh, 1997).

Role of Computers and the Literature

Eventually, Flannery would also reveal her cryptosystem to the mathematical public to have them search for holes, but first she had to search for some possible attacks herself. Toward this end, she had to "go to the journals" to search for as many articles with descriptions of relevant methods of attack as she could find. The literature in journals is one of the essential tools that mathematicians use to develop further knowledge because it exposes them to other scholars' ideas, progress, and proof techniques. To illustrate how important this tool is, the author cites the story of Gauss who apparently chose to attend Göttingen University rather than another school because the library was better (Flannery, 2001).

Another tool that Flannery relied on heavily was computer programming. As she was

culling the literature, she would program in the language Mathematica to get a better understanding of certain attacks as well as simple mathematical theorems by generating multiple examples (Flannery, 2001). This type of programming plays a significant role in modern mathematics because the ability to easily manipulate multiple examples can greatly build mathematical intuition.

Conclusion

The final phase of Flannery's mathematical journey was the presentation of her algorithm at Ireland's Young Scientist Exhibition, where it was met with incredible praise and generated an international media blitz. In the end, though, her work succumbed to the same fate of Cauchy and Lamé. An attack was eventually found by a cryptographer reviewing her work, and despite her attempts to find a patch, no method was found to salvage the cryptosystem (Flannery, 2001). This experience provides further insight into the course of knowledge development in mathematics by demonstrating the potential fallibility of mathematical claims that have no clear proofs, as well as the cycle of review and revision that mathematical claims must undergo. Finally, this story also highlights the primary criterion for when knowledge will become accepted as true, namely that it pass the scrutinizing review of the mathematical community at large.

References

- Flannery, S. with Flannery, D. (2001). *In Code: A mathematical journey*. New York: Workman Publishing Company.
- Singh, S. (1997). *Fermat's Enigma: The epic quest to solve the world's greatest mathematical problem*. New York: Anchor Books.