Book Review

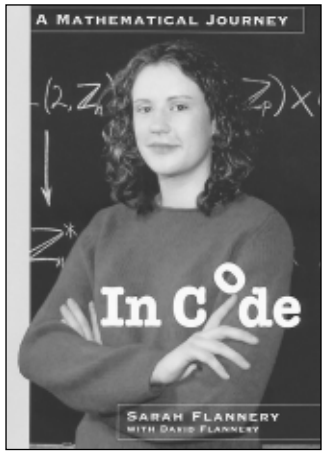
In Code: A Mathematical Journey

Reviewed by Rafe Jones

In Code: A Mathematical Journey
Sarah Flannery and David Flannery
Workman Publishing Company, 2001
265 pages, $24.95, ISBN 0-7611-2384-9

I can imagine three principal reasons for a mathematician to read Sarah Flannery's book *In Code*: first, for insight into the thoughts of a teenager who did one very good piece of mathematical work and found herself suddenly famous for it; second, for a lively introduction to public-key cryptography and, more specifically, the RSA algorithm and the alternate algorithm the author created; and, finally, for simple enjoyment. Though it is strongest on the first point, the book delivers much in all three of these areas.

Though one might expect a degree of smugness in a book written by a teenager about her mathematical exploits, there is not a trace of it here. Rather than focusing on Sarah's accomplishments right away, the book opens with a few pages of family background, followed by a fairly lengthy section titled "Early Challenges". This consists of descriptions and solutions of about a dozen mathematical puzzles given to Sarah and her brothers in their childhood by their father and mathematical mentor, David Flannery. Following the descriptions of each puzzle are exhortations to the reader to try them out before continuing to their solutions. I found myself wanting to solve all the puzzles before reading the answers, though I was not always successful. This puzzle series serves as a warm invitation to the reader to participate in the text, the very opposite of an off-putting narrative of triumph. Even when the book comes around to giving an account of her prizes and publicity, Sarah remains steadfastly humble. "I have no doubt that I am not a genius," she declares. "I am not being falsely modest. Through my father's classes I have seen examples of true genius, and I know I do not possess that 'insight' that distinguishes geniuses from those regarded as merely intelligent" (p. 243). In the face of such mathematical enthusiasm and humility, I felt compelled to root for Sarah, even though I knew her eventual success was assured.



After the puzzle section comes a description of the origins of the very good piece of work that would result in Sarah's sudden fame. When she attempts to think of a suitable subject for a project to be entered in the 1998 Esat Irish Young Scientist competition (akin to a national science fair), her father proposes that she do a project on cryptography. They decide that her project will explain various cryptographic techniques, culminating in an account of the famous RSA algorithm. Sarah discusses learning the relevant mathematics and doing the necessary programming. But the story stops there—on page 40—and does not resume for nearly 150 pages. The pages between are filled with an engaging, though lengthy, mathematical exposition written largely by David Flannery. It details the ideas necessary for a basic understanding of public-key cryptography in general and the RSA algorithm in particular.

When Sarah's story does resume, she is in the final days of preparing for the 1998 Young Scientist contest. The project earns several prizes and spurs her to undertake a more ambitious entry the

Rafe Jones is a graduate student in mathematics at Brown University. His email address is jones@math.brown.edu.

following year. Inspired by techniques she encounters in a week-long internship at a Dublin cryptography company, she devises an alternate algorithm to the RSA and makes it the centerpiece of her new project. Based on simple matrix multiplication rather than the relatively cumbersome modular exponentiation of the RSA, her algorithm runs nearly twenty times faster. She names it the Cayley-Purser algorithm, after Arthur Cayley, the nineteenth-century British mathematician, and Michael Purser, the mathematician whose ideas she encountered during her internship. Proving that the new algorithm is secure from certain kinds of attacks becomes a mathematical odyssey for the youngster, requiring her to explore and master a labyrinth of unfamiliar mathematics.

Her account of this process of discovery reminded me of the better moments I've had in graduate school. "All of this was an unusual experience for me," she writes, "but I had a great feeling of excitement. I think it was because I was working on something that no one had worked on before. I worked constantly for whole days on end, and it was exhilarating" (p. 208). Reading these pages gave me an infusion of excitement about my own thesis problem—I suddenly felt remarkably fortunate to have a problem of my very own. I made a sincere (though short-lived) resolution to work extra, extra hard on it.

Eventually Sarah is successful in showing the Cayley-Purser algorithm is immune to a large family of attacks. She writes a vivid account of the judging of her new project, which explains the algorithm and proof, in the 1999 Irish Young Scientist competition. Quoting directly from her journal, she conjures feelings that I can remember from my own high school science fair project on methods of computing π. "On one occasion," she writes, "I looked out of our little huddle and it felt really strange—our conversation was so very intense that just to look around was like coming up for air" (p. 222). On her best moment of the judging, she writes: "Before they left, [the judge] asked me the simplest question of all, and I could see he was wondering whether or not I would be able to answer it. The answer was the fast exponentiation algorithm, and I must have smiled before I replied, because I knew it was the perfect end to the perfect session. I had been able to defend my project at all levels. The last question was a check to see if I knew the fundamentals. They smiled at each other on my final answer, which I'll never forget" (p. 223).

Two days later Sarah walks up to the awards stage to accept the title of Irish Young Scientist of the Year. With her youth and the theoretical possibility of riches her algorithm holds out, the general news media takes notice. Thanks to the unexpected front-paging of a *London Times* article on her exploits, she becomes an overnight sensation. Over the next few months she receives, among other things, multiple offers from would-be cryptography entrepreneurs, an invitation to give a series of lectures in Singapore, a mention in the official magazine of the Spice Girls, and a request from Profile Books in London to write up her experiences and background in book form.

The story's final twist comes when Michael Purser alerts her to a seemingly lethal kind of attack on the Cayley-Purser algorithm. Though Sarah strives to repair her algorithm, she does not succeed and finally concludes it is not salvageable as a workable encryption system. But its theoretical interest persists. Though she includes a postscript on the successful attack, her project nevertheless earns her the title of European Young Scientist of the Year for 1999.

The mathematical part of the book is almost entirely separate from the two narrative segments at the beginning and the end, and therein lies the book's main flaw. Though skillfully written, the nearly 150 pages of mathematics separating the story's beginning and end is simply too much and makes it difficult to get a good chronological sense of the events of Sarah's life. While reading the mathematical section, I frequently wondered where the book was going and what its exact structure was. I should note, though, that the authors likely felt compelled not to intersperse the mathematical exposition with bits of narrative in order to accommodate readers who do not want to read much of the mathematics.

Taken alone, the mathematical exposition is lively and accessible. It begins with an elementary examination of prime numbers that virtually any reader should be able to follow. After an introduction to the idea of primality, sections on Mersenne primes, the Sieve of Eratosthenes, and primality testing make up the main attractions. Then comes a slightly more difficult chapter devoted mainly to describing the Caesar cipher and its generalizations. Following this is a much more advanced, though still elementary, chapter dedicated mainly to modular arithmetic, Fermat's Little Theorem, and pseudoprimes. Though the latter two of these three mathematical chapters are necessary for a full understanding of the RSA algorithm, they can be safely skipped by readers who wish to acquire only a basic feel for public-key cryptography. The next two chapters deal with one-way functions and the RSA algorithm, respectively. They are written in plain English with lucid explanations and should hold some appeal for all readers.

The authors have taken pains to make the book mathematically engaging and accessible and to paint a picture of mathematical thought as playful and evolving. Because of this and the large element of human interest that is in Sarah's warm, enthusiastic account of her experiences, *In Code* makes good reading for the mathematically curious of all ages.