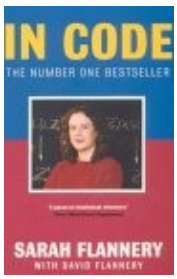
March 2001
Reviews

'In Code'

reviewed by Helen Joyce



In Code − a Mathematical Journey

"...puzzles have been far more beneficial to me than years of learning formulae and 'proofs'."

Sarah Flannery

This is the story of Sarah Flannery, who at age 16 won the titles of 1999 Irish Young Scientist of the Year and European Young Scientist of the Year for her innovative work on cryptography. Written by Sarah with her father David, who taught her mathematics from a young age and encouraged her mathematical flights, the book is an engaging mix of mathematical exposition − always clear and rigorous but never dull − and first−person descriptions of the storm that erupted when the world media latched onto her story. Easily written in a friendly style, you could imagine that this is the adventure of someone you know.

Sarah has clearly not got over the extraordinary way things developed after she won these prizes. In many ways she comes across as a very ordinary down−to−earth person who found herself in an extraordinary situation. This is of course not quite accurate, because she is clearly more capable, hardworking and courageous than most. She also comes across as very likeable, which she might very well not have, given that the book is a first−person account of her successes − never an easy genre.

A strength of the book is its touching description of the process of discovering what mathematics really is, and how it feels to do some real maths for the first time in your life. As Sarah says herself, "there is a lot of difference between, on the one hand, listening to maths being talked about by somebody else and thinking that you are understanding, and, on the other, thinking about maths and understanding it yourself and talking about

it to somebody else".

It is a tribute to the author that this book is inspiring rather than intimidating. Sarah clearly doesn't hold herself back − I don't mean that she is brashly overconfident, just that she doesn't let her worries and insecurities get in the way of her thinking and the work she is doing.

Briefly, Sarah's extraordinary story is this.

Interested in maths from a young age, and encouraged by her father David, who lectures in mathematics, Sarah became interested in cryptography when attending an evening mathematics enrichment class given by her father. Inspired by the course, she arranged to do one week's work experience at Baltimore Technologies, a cryptography firm in Dublin founded by Dr Michael Purser.

A number of years ago, Dr Purser spent some free time trying to find a new cipher. It didn't really work for what he was interested in at the time, which was digital signatures, but did seem to be useable for public key cryptography. It was based upon quaternions.

Dr Purser did as he usually did with such ideas − wrote it up and filed it away. Then, while he was away on holiday, Sarah turned up for her work experience. The first day was a bank holiday, and on the second day she made tea. On the third day the staff realised she was capable of doing more, and so she was given the work Dr Purser had written up to program, which she spent the rest of the week doing.

Dr Purser only met Sarah for the first time three months later, when she explained some alterations she was making to his cipher idea, in particular working with 2x2 matrices instead of quaternions. Then, according to Dr Purser, "there was a long silence, and then a breathless phone call from Sarah, saying "I've won first prize!' What first prize? I hadn't even known she had entered a competition!" (The prize was for Irish Young Scientist of the Year 1999.)

The work Sarah entered for the competition was an enormous amount of background research into cryptography, as well as some original work of her own on a cipher she thought could be used for public key cryptography, based on Dr Purser's original idea. The press picked up on the story, and Sarah spent a lot of time travelling and lecturing, and there was even talk of her patenting her cipher − which Dr Purser advised her against.

As Dr Purser explains, it was at this point that he and William Whyte (chief cryptographer at Baltimore Technologies) became worried that the cipher had a flaw in it. Since the work had originated at Baltimore Technologies, it was possible the company would be held liable for any ensuing losses. Sadly, their worries were well−founded. An obscure flaw meant that the code − named the Cayley−Purser code for early cryptographer Cayley and Dr Purser − could not be used as it stood for public key cryptography. Sarah and David Flannery, together with Michael Purser and William Whyte, spent some time trying to rectify the problem, but they never succeeded, so the algorithm as it stands is defective. Sarah decided her best course was to publish, pointing out the defects.

After the hectic years described in "In Code", Sarah is now doing a degree in maths and computer science, and trying to live the life of a normal young student.

Book details:

In Code − A Mathematical Journey
Sarah Flannery with David Flannery
Paperback − 288 pages (February 2001)
Profile Books

ISBN 1861972717

Plus is part of the family of activities in the Millennium Mathematics Project, which also includes the NRICH and MOTIVATE sites.