Irish Math. Soc. Bulletin
Number 76, Winter 2015, 79–81
ISSN 0791-5578

D. Rosenthal, D. Rosenthal and P. Rosenthal: A Readable Introduction to Real Mathematics, Springer, 2014. ISBN:978-3-319-05653-1, ebook GBP 27.99, hardcover GBP 35.99, 161+xii pp.

REVIEWED BY ROBIN HARTE

This book comes with a public health warning: very hard to put down. Contrary to the impression given by its possibly over-loud title - probably deriving from the excitement of the bridging course in Toronto - this book is basically a new and refreshing introduction to number theory. In outline, in twelve chapters, it progresses from the natural numbers and induction through modular arithmetic, the "fundamental theorem of arithmetic" and the Euclidean algorithm to the RSA method of public key encryption. After a look at complex numbers and the cardinality of infinite sets, it goes on to discuss "plane geometry", ruler-and-compass constructibility, and surds. But the heart of it is the number theory: prime factorization, the ϕ function, the Euclidean algorithm, Fermat's and Wilson's theorem, here put to work in the service of RSA and public key encryption. This reviewer has always been a little afraid of number theory: all that stuff about phi functions and prime number density has seemed arcane and irrelevant, very far away from "real mathematics". Now. after immersing himself in this little book, number theory begins to make sense.

"Uncle Petros", fronting for Apostolos Doxiadis [1], tells his nephew that "addition is natural, but multiplication is artificial". To see what he is getting at just, on day two of your introductory course, write out the first few natural numbers in factorized form:

$$1, 2, 3, 2^2, 5, 2 \cdot 3, 7, 2^3, 3^2, 2 \cdot 5, 11, 2^2 3, 13, 2 \cdot 7, 3 \cdot 5, 2^4, 17, 2 \cdot 3^2, 19 \ :$$

is there any discernible pattern? Number theory is born out of the attempt to answer that question.

Peter Rosenthal - who with Heydar Radjavi wrote the book on invariant subspaces - has with his extended family come down to

Received on 20-11-2015.

©2015 Irish Mathematical Society

earth with a vengeance and struck bedrock. All about natural numbers and prime factorization, a conversational style of writing conceals some very serious mathematics. The fundamental role of the Euclidean algorithm permeates the account: things are sometimes proved twice, first without and then with its help. There is a succinct account of Public Key Cryptography and RSA, which with our obsession with internet security has made number theory cool, introduced [2] to an Irish audience by our own mathematical family of Sarah Flannery and Dave; the arcane Fermat and Wilson theorems are put to work reach "encryptors" and "decryptors", either with or without the help of the Euclidean algorithm. Modular arithmetic leads to the "Chinese remainder theorem" which is buried in an INTEL chip, and to tests for divisibility by 9, 11 and indeed 7: for example the serial number of an Irish euro note, beginning with the letter T , is always equal to 6 mod 9, and the serial number T39484135244 would therefore suggest forgery.

For serendipity it will be hard to beat the identification of ruler-and-compass constructible numbers with "surds", here given a rather careful definition. This reviewer however wonders whether these surds should more properly be called "quadratic surds", in that it not immediately obvious whether or not the cube root of two is such a thing. He is also reassured to see that the constructions are carried out in "numerical space" $\mathbb{R}^2$ rather than some "Euclidean geometry" of whose foundations he would be unsure. The authors are careful to frighten nobody: but they could afford to incorporate a carefully sealed-off appendix listing axioms for the real number system $\mathbb{R}$, and at one point to offer a simple statement of the terrifying Gelfond-Schneider theorem. They could also tell us that the "natural numbers" are in a sense *defined by induction*: Bertrand Russell explained [3] that from his prison cell as a conscientious objector.

Having taken by the scruff of its neck the half-defined word "surd" and given it a specific meaning of their own, the Rosenthals could also do the same for the honorary real number ∞, which to us represents the smallest infinite cardinal, coinciding with the first infinite ordinal:

$$\mathbb{N} = \{1, 2, 3, \ldots\} \subseteq \infty = \{0, 1, 2, \ldots\} \subseteq \infty + 1 = \infty \cup \{\infty\};$$

only now do we introduce the inscrutable "function" $\aleph : n \mapsto \aleph_n$ from ordinals to cardinals, for which

$$\aleph_0 = \infty < \aleph_1 \leq |\mathbb{R}| = 2^\infty = \aleph_k \ ,$$

where the status of the ordinal k is one of the great mysteries of mathematics.

There are just one or two dropped stitches: for example the product

$$100,000,559 = 53 \cdot 223 \cdot 8461$$

is offered as an example of a prime number, and technology has now caught up with their $3 + 2^{3,000,005}$. It is perhaps not entirely clear what the intended audience would make of this book if left to read it on their own: but to this rather jaded ex operator theorist it begins to make sense of all that "number theory" he never could get to grips with.

References

[1] Apostolos Doxiadis, Uncle Petros and Goldbach's conjecture, 1992.
[2] Sarah Flannery, In code: a mathematical journey, 2001.
[3] Bertrand Russell, The Principles of mathematics, Norton, 1903.

Robin Harte Still loosely attached to TCD, Robin is the author of *Spectral mapping theorems, a bluffer's guide* (Springer briefs in mathematics, 2014), and also of *Invertibility and Singularity* (Dekker 1988), now shortly to be re-released by Dover Books.

School of Mathematics, TCD
E-mail address: hartere@gmail.com