The Book Review Column[1]

by Frederic Green

Department of Mathematics and Computer Science
Clark University
Worcester, MA 01610
email: fgreen@clarku.edu

In this column we review three accessible books about difficult subjects. The second and third are in the AMS Student Mathematical Library, a series I have so far found to be uniformly excellent.

1. **Q is for Quantum**, by Terry Rudolph. An explanation of the puzzling nature of quantum mechanics with no mathematical (or physical) prerequisites. Review by Bill Gasarch.

2. **An Introduction to Ramsey Theory: Fast Functions, Infinity, and Metamathematics**, by Matthew Katz and Jan Reimann. An introduction which includes a proof that a *natural* statement (in Ramsey Theory) is not provable in Peano Arithmetic. Review by Bill Gasarch.

3. **Modern Cryptography and Elliptic Curves, A Beginner's Guide**, by Thomas R. Shemanske. An introduction to this fascinating area of mathematics, with applications to cryptography. Review by Frederic Green (third installment in my series on number theory).

Please drop me a line if you'd like to write a review; choose from among the books listed on the next pages, or, if you are interested in anything not on the list, just send me a note.

BOOKS THAT NEED REVIEWERS FOR THE SIGACT NEWS COLUMN

Algorithms

1. *Tractability: Practical approach to Hard Problems*, Edited by Bordeaux, Hamadi, Kohli
2. *Recent progress in the Boolean Domain*, Edited by Bernd Steinbach
3. *Finite Elements: Theory and Algorithms*, by Sahikumaar Ganesan and Lutz Tobiska
4. *Introduction to Property Testing*, by Oded Goldreich.
5. *Algorithmic Aspects of Machine Learning*, by Ankur Moitra.

Miscellaneous Computer Science

1. *Elements of Causal Inference: Foundations and Learning Algorithms*, by Jonas Peters, Dominik Janzing, and Bernhard Schölkopf.
2. *Elements of Parallel Computing*, by Eric Aubanel
3. *CoCo: The colorful history of Tandy's Underdog Computer* by Boisy Pitre and Bill Loguidice
4. *Introduction to Reversible Computing*, by Kalyan S. Perumalla
5. *A Short Course in Computational Geometry and Topology*, by Herbert Edelsbrunner
6. *Partially Observed Markov Decision Processes,* by Vikram Krishnamurthy
7. *Statistical Modeling and Machine Learning for Molecular Biology*, by Alan Moses
8. *The Problem With Software: Why Smart Engineers Write Bad Code,* by Adam Barr.
9. *Language, Cognition, and Computational Models,* Theirry Poibeau and Aline Villavicencio, eds.

Computability, Complexity, Logic

1. *The Foundations of Computability Theory,* by Borut Robič
2. *Applied Logic for Computer Scientists: Computational Deduction and Formal Proofs*, by Mauricio Ayala-Rincón and Flávio L.C. de Moura.
3. *Descriptive Complexity, Canonisation, and Definable Graph Structure Theory*, by Martin Grohe.
4. *Kernelization: Theory of Parameterized Preprocessing,* by Fedor V. Fomin, Daniel Lokshtanov, Saket Saurabh, and Meirav Zehavi.

Cryptography and Security

1. *Cryptography in Constant Parallel Time,* by Benny Appelbaum
2. *Secure Multiparty Computation and Secret Sharing*, Ronald Cramer, Ivan Bjerre Damgård, and Jesper Buus Nielsen
3. *A Cryptography Primer: Secrets and Promises*, by Philip N. Klein

Combinatorics and Graph Theory

1. *Finite Geometry and Combinatorial Applications*, by Simeon Ball
2. *Introduction to Random Graphs*, by Alan Frieze and Michał Karoński

3. *Erdős –Ko–Rado Theorems: Algebraic Approaches*, by Christopher Godsil and Karen Meagher
4. *Combinatorics, Words and Symbolic Dynamics,* Edited by Valérie Berthé and Michel Rigo

Miscellaneous Mathematics

1. *Introduction to Probability*, by David F. Anderson, Timo Seppäläinen, and Benedek Valkó.

Review of[2]
Q is for Quantum
by Terry Rudolph
Terence Rudolph, 2017
164 pages, Softcover, $12.99.

Review by
William Gasarch (gasarch@cs.umd.edu)
Department of Computer Science
University of Maryland, College Park, MD

1 Introduction

Fred Green asked me to review two books for opposite reasons.

- *Fred:* Bill, could you review **An Introduction to Ramsey Theory: Fast Functions, Infinity, and Metamathematics** by Matthew Katz and Jan Reimann since you are an expert on Ramsey Theory.

  Bill: I WOULD NOT say I am an expert, but sure, I can review that.

- *Fred:* Bill, could you review **Q is for Quantum** by Terry Rudolph. It's aimed at people who know NOTHING about quantum mechanics and don't know that much math, so I thought of you.

  Bill: I WOULD say I know nothing about quantum and don't know that much math, so sure, I can review it.

This book really is written for people who know NOTHING about quantum mechanics and don't know much math, hence I was able to give it a fair review. Since I have sometimes heard people talk about quantum mechanics I could also recognize some of the discussions in the book as well known controversies in quantum mechanics.

I first thought this book would take Scott Aaronson's approach of starting with a very strange way to do probability. But even that is more math than this book wants to do. Instead the book describes very tangible but impossible-sounding devices whose macro-level behaviour is known and which really can be built, although there are controversies about what they are really doing on the micro level.

2 Summary of Contents

Part 1: Q-computing

The author describes a variety of devices where you drop white and black balls into them and some other (or the same) color balls come out of them. These are circuits though he does not use the term. Most of them are ordinary:

1. A NOT box: input a white ball, get out a black ball, and vice versa.

2. A SWAP box: BB goes to BB, BW goes to WB, WB goes to BW, WW goes to WW.

[2]

3. A CNOT (Controlled NOT): if the first ball is W then the second ball stays the same. If the first ball is B then the second ball changes color.

4. There are others.

He then introduces the PETE box.

1. If you input a white ball then with probability $\frac{1}{2}$ you get a white ball, and with probability $\frac{1}{2}$ you get a black ball.

2. If you input a black ball then with probability $\frac{1}{2}$ you get a white ball, and with probability $\frac{1}{2}$ you get a black ball.

That doesn't look so unusual. The PETE box obviously flips a coin or some such. Nothing to see here, move along folks.

Not so fast! If a ball goes through one PETE box and then the output to another PETE box (no peeking at what happens after the first PETE box!) then you *should* get, no matter which color ball you drop in, $P(W) = P(B) = \frac{1}{2}$. But you don't!

1. If you input a white ball through two PETE boxes you end up with a white ball. ALWAYS!

2. If you input a black ball through two PETE boxes you end up with a black ball. ALWAYS!

Well isn't that odd? It gets odder: (1) If you DO peek then the behavior stops, and (2) PETE boxes seem to really exist in nature. And people can build them. And they are useful in the real world. The question of what is going and how they work leads to that old saw:

$1 + i$ *quantum mechanics,* $2 + 2i$ *opinions.*

He explains this behavior in terms of the balls not really being white or black but being what he calls *misty balls* and what physicists call *a superposition of white and black*. So the ball's color is really something like $(W, -B)$. The key to the behavior is that negatives and positives can cancel out.

He then explains how you can use these misty balls to do all kinds of wonderful computations (he does not explain factoring, which makes sense given the math he assumes of the audience). Interwoven is some debate on whether the model is TRUE or just GOOD FOR CALCULATION BUT NOT REALLY TRUE which mirrors a current debate within the physics community.

He is very careful NOT to say that a quantum computer visits an exponential number of options at one time, but instead to point to the canceling out as why these devices are powerful. I applaud this.

Part 2: Q-Entanglement

This Part begins by talking about alleged psychics Alice and Bob. Alice is in a room with tester ONE, Bob is in a room with tester TWO. Both testers flip a coin. After the coin flip Alice and Bob each say B or W (Black or White). We denote the coins they see by (Alice's coin, Bob's Coin).

- If HH then Alice and Bob say BW, WB, or WW to be okay. If they say BB then DOOM!

- If HT then Alice and Bob say BB, BW, or WW. If they say WB then DOOM!

- If TH then Alice and Bob say BB, WB, or WW. If they say BW then DOOM!

- If TT then Alice and Bob say BB, WB, or WW. If they say BB then they WIN!

If Alice and Bob want to take no chance on DOOM then because they can't know the other person's coin flip, it also appears they have no chance of ever winning. But the author shows that if both take lots of balls and a PETE box in their room they CAN always avoid DOOM yet still win some of the time. So quantum entanglement is tied to these PETE boxes.

Part 3: Q-Reality

Throughout the book there were some side comments about what is really going on. Part 3 expands on these notions. Many different points of view are presented to try to explain what is going on here. No conclusion is reached.

3 Opinion

I was going to write that this book is a great starting point to help you *understand* quantum mechanics. Then I read the following quote attributed to Richard Feynman:

> *There was a time when the newspapers said that only twelve men understood the theory of relativity*[3]*. I do not believe there was ever such a time. There might have been a time when only one man did, because he was the only guy who caught on, before he wrote his paper. But after people read the paper, a lot of people understood the theory of relativity one some way or other, certainly more than twelve. On the other hand, I think we can safely say that nobody understands quantum mechanics.*

So it's not just laypeople who don't understand quantum mechanics. Even physicists don't!

This book is excellent at explaining what is so strange about quantum mechanics without getting technical, without using mathematics beyond high school algebra, and without saying things I never quite understood like *the cat is alive and dead!* or *It's a wave! It's a particle! It's a desert topping! It's a floor wax!* They do talk some about *once you look at something, it changes* but they do this in an intelligent way that is understandable. So it tells the the layperson what it is about quantum mechanics that people, even physicists, don't understand.

When I finished reading the book I wanted to learn more (a sign of a good book). There is a website associated to the book

`www.qisforquantum.org`

which has some recommended books to read next.

[3] I wonder how many women did.

Review of[4]
An Introduction to Ramsey Theory:
Fast Functions, Infinity, and Metamathematics
by Matthew Katz and Jan Reimann
AMS, 2018
207 pages, Softcover, $52.

Review by
William Gasarch (gasarch@cs.umd.edu**)**
Department of Computer Science
University of Maryland, College Park, MD

1 Introduction

The first theorem in Ramsey Theory is:

> For all 2-colorings of the edges of K_6 there is a monochromatic K_3.

This generalizes to the first real theorem:

> For all m there exists $R = R(m)$ such that, for all 2-colorings of the edges of K_R there is a monochromatic K_m.

More generally, Ramsey theory is a branch of combinatorics that deals with statements of the form

> If you color a large enough BLAH you will have a nice monochromatic sub-BLAH.

The book under review is at first a standard book on Ramsey Theory, but which then takes a turn into connections to logic. Logic? Where does logic come in?

Recall Gödel's incompleteness theorem which we summarize as:

> There are statements S such that S is true of the natural numbers but cannot be proven in Peano Arithmetic.

This is a very important theorem since it shows that Peano Arithmetic cannot do everything in Number Theory. However, the statement S is not natural. Paris and Harrington came up with a natural statement in Ramsey Theory that is not provable in Peano Arithmetic. I have always wanted a clean self-contained treatment of the Paris-Harrington result and why it is not provable in Peano Arithmetic. Is this book that treatment? Yes!

We give some definitions that we use throughout the review:

Definition

1. PA is Peano Arithmetic. It is a system of axioms and rules of inference. Most theorems in number theory can be proven in it. Almost all (all but a finite number :-)) interesting theorems in number theory can be proven in it.
2. If ϕ is a statement that can be proven in PA then we write $PA \vdash \phi$. Note that ϕ must be written in the language of PA.

3. If ϕ is a statement and it cannot be proven in PA then we write $PA \nvdash \phi$. Note that ϕ must be written in the language of PA. If ϕ was a theorem in analysis (e.g., the intermediate value theorem) then technically $PA \nvdash \phi$ is true but one would never write that.

4. PH is the Paris-Harrington statement which I will define later in this review.

Definition: Let $k, n \in \mathbb{N}$. Then $[n]$ denotes the set $\{1, \ldots, n\}$, and $\binom{[n]}{k}$ is the set of all k-sets of $[n]$. $\binom{\mathbb{N}}{k}$ is the set of all k-sets of $\mathbb{N}$.
Definition: Let $c \in \mathbb{N}$ and let COL be a c-coloring of $\binom{[n]}{k}$ (respectively $\binom{\mathbb{N}}{k}$). We say $H \subseteq [n]$ (respectively $H \subseteq \mathbb{N}$) is *homogenous with respect to* COL if all elements of $\binom{H}{k}$ are the same color.

2 Summary of Contents

Chapter 1 is mostly standard material on Finite Ramsey Theory. We state Ramsey's Theorem for hypergraphs, which is one of the results they prove.

> **Ramsey's Theorem for Hypergraphs:** For all c, k, m, there exists n such that for all c-colorings of $\binom{[n]}{k}$ there is a homogenous set of size m.

The book gives proofs, upper bounds on n, and lower bounds on n. The lower bounds were shown by the probabilistic method. One could say this is an application of the probabilistic method but that's a bit odd since the probabilistic method was originally invented by Paul Erdős for this purpose. The authors also give a proof of Ramsey's Theorem (for hypergraphs) by Nesetril which is more abstract and new (at least to me).

Chapter 2 is about the infinite Ramsey Theorem:

> **Ramsey's Theorem for Infinite Hypergraphs:** For all c, k, for all c-colorings of $\binom{\mathbb{N}}{k}$, there is an infinite homogenous set.

This can be proved directly, or from the finite Ramsey Theorem. Alternatively one can prove the finite Ramsey Theorem from the infinite. This chapter looks at variants of this on cardinals and large cardinals.

Chapter 3 is about the Growth of Ramsey Numbers
We state van der Waerden's (VDW) Theorem:

> **Theorem:** For all c, k there exists $W = W(k, c)$ such that for all c-colorings of $[W]$ there exists a, d such that a, $a + d$, …, $a + (k - 1)d$ are all the same color. (A monochromatic arithmetic sequence.)

They present the original proof that gives Ginormous bounds on $W(k, c)$. They then give Shelah's' proof of the Hales-Jewitt Theorem which yields much smaller bounds on $W(k, c)$. They don't seem to mention (unless I missed it) that Gowers gave a proof with even smaller bounds. If this is their example of a large growing Ramsey function it's not quite right. The proof of VDW's Theorem does give a bound that grows very fast, but what it is bounding ends up not being that fast growing. The distinction should have been made more clear. Having said all that, this is a fine presentation of the proofs given.
They also prove the Paris-Harrington (PH) Ramsey Theorem:

Definition: A *large set* is a finite set of $\mathbb{N}$ where the size of the set is bigger than the smallest element.

One might wonder if you can get a homogenous set that's large. That's not quite right since if 1 is in the set then it's already homogenous. But what if you start the numbering of the vertices with a larger number? With that in mind:

> **PH Ramsey's Theorem for Hypergraphs:** For all c, k, there exists n such that for all c-colorings of $\binom{\{k,k+1,\ldots,k+n\}}{k}$ there is a large homogenous set of size m. We denote m by $PH(k, c)$.

One way to prove this is from the Infinite Ramsey Theorem. This proof does not give any bounds on n. Is there a proof that gives bounds on n? See Chapter 4.

Chapter 4 is the proof that $PA \nvdash PH$. One consequence of this is that there is no proof that gives bounds on $PH(k, c)$.

There are two ways to prove $PA \nvdash PH$. One way is to show that the PH function grows so quickly that it can't be proven to exist in PA. The other way is to use non-standard models of PA, indiscernibles, and, ironically, Ramsey Theory! That is the way the authors proved it. Their presentation is self-contained and can be followed by a non-logician. It will take some time to get through but is well worth it.

3 Opinion

This is a great book! This finally gives me the self-contained treatment of $PA \nvdash PH$ that I feared I would have to write myself if someone else didn't write it. It is well written and gives the reader just enough logic to understand the proof.

I consider the $PA \nvdash PH$ to be the point and highpoint and purpose of the book. However, there is other good material in there as well on both Ramsey Theory and Logic.

Who should read this book? Who shouldn't read this book?

Alice is thinking of reading this book. Alice's knowledge of Ramsey Theory is α, and of logic is β. Alice's mathematical maturity is γ. We take $\alpha, \beta, \gamma \in \{0, 1, \ldots, 100\}$. For what values of α, β, γ should Alice read this book? Clearly for $(\alpha + \beta)\gamma \geq 150$. I am, of course, kidding.

If Alice knows some Ramsey Theory but little logic, she can skim the Ramsey Theory and learn logic. She won't just learn the logic needed for $PA \nvdash PH$, she will also learn about large cardinals, ordinals, and some non-standard models of PA. She will even learn how to apply Ramsey theory to logic.

If Alice knows some logic but little Ramsey Theory she can skim the logic and learn Ramsey Theory. She won't just learn Ramsey Theory. She will learn about the interactions of Ramsey Theory to her field of Logic.

If Alice knows neither but has lots of math maturity she could read and understand the book, though it will be a tough read.

Only if Alice lacks knowledge and maturity would this book be too hard for her.

Review of[5]
Modern Cryptography and Elliptic Curves, A Beginner's Guide
by Thomas R. Shemanske
AMS, 2017
252 pages, Softcover, $52.

Review by
Frederic Green (fgreen@clarku.edu)
Department of Mathematics and Computer Science
Clark University, Worcester, MA

1 Introduction

The equation $y^2 = x^3 + ax^2 + bx + c$ might seem a little innocuous at first. However, studying the sets of rational points (x, y) obeying this equation has proven to be one of the most far-reaching and fruitful areas of mathematics. For example, it led, aided and abetted by much of the most powerful mathematics of the past century, to Wiles' proof of Fermat's Last Theorem. And furthermore, these so-called "elliptic curves" (the terminology having little to do with ellipses) are actually *useful*. You can factor numbers with them! And send secret messages!

The present book introduces the reader to elliptic curves as well as their application to cryptography. As the prerequisites are very minimal, it actually does a great deal more in the process. This is a tall order, and I'll cut to the chase: This is an excellent book! But before I attempt to justify that statement, let's look at what's in the book.

2 Contents

The first chapter briefly discusses two famous problems, Fermat's Last Theorem and the Congruent Number Problem (which natural numbers equal the area of some right triangle with rational sides?), and the central application, cryptography. The second chapter goes into the very basics of elementary number theory, enumerating Pythagorean Triples, exploring connections between geometry and algebra, and taking a quick peek ahead at the seemingly magical algebraic properties of elliptic curves. (Anyone reading this book at this point *cannot* pass up the opportunity to work out Bachet's duplication formula for $y^2 = x^3 + k$!) Chapter 3 lays further foundations of elementary number theory, e.g., congruences, modular arithmetic, Euclid's algorithm, Chinese remaindering, and an application in the form of affine ciphers. We get into algebra more deeply in Chapter 4, with more on congruences, groups, rings, and fields. The reader is not assumed to be familiar with equivalence relations, so they are explained too. Also studied are the structure of $\mathbb{Z}_n$, its group of units U_n, Euler's theorem on the totient alongside its ubiquitous consequence Fermat's little theorem, and applications to factoring, in particular Pollard's $p - 1$ method.

In Chapter 5, we move on to cryptography in general. The introduction is enlivened by real-world scenarios of what happens under the hood when you send privileged information over Wifi in a coffeeshop. The presentation focusses on RSA, drawing on the background of the previous chapters. However, it describes further practical aspects of cryptographic protocols, including authentication and the role of hash functions. There is a very nice discussion of hashing in general, given a real-world context outside of cryptography.

And, in learning the contrast between the collision and second preimage resistance criteria for hashing, we get to take a detour to the birthday paradox. The chapter ends with a brief discussion of crytanalysis, largely from the RSA standpoint.

Chapter 6 returns to algebra, focusing on group theory. After the requisite introduction to group homomorphisms, cyclic groups, and direct products, there is an exposition (with no proofs) of the classification of the finite abelian groups. A discussion of primitive roots leads naturally into expositions of Diffie-Hellman and ElGamal encryption.

Chapter 7, mathematically the most substantial, wisely confines itself to elliptic curves alone. Elliptic curves over $\mathbb{R}$ are emphasized for intuition. Here all the preceding spadework truly pays off. The first order of business is to explain projective space, which leverages the prior attention to equivalence relations. It doesn't just *define* projective space, but also explains *why* things work as they do, for example, why we need homogeneous polynomials (stopping just short of introducing homogeneous coordinates). There follows one of the more lengthy and involved sections, on the group law for elliptic curves, but taking the reader through not-quite-correct initial attempts, explaining why they fall short of the goal, and thereby, step by step, motivating the correct definitions. While the group law isn't proved in all generality, a standard (convincing enough!) geometric overview of the associative property (the hard part) is given. Explicit formulas for the group law, crucial for computation, are also derived. (One could prove associativity via very tedious calculation from these formulas, something the beginner might or might not want to do, or, as outlined later in the appendix, an elegant proof is outlined in the context of elliptic curves over $\mathbb{C}$.) The chapter ends with a brief discussion of Hasse's bound on the number of points in an elliptic curve over a finite field, also crucial for cryptography. This also provides an opportunity to introduce quadratic residues.

Chapter 8 presents the two applications central to the theme of the book. The first is Lenstra's elliptic curve method for factoring. This is done by analogy with Pollard's $p-1$-method, with careful attention to the similarities and differences (e.g., Pollard's method relies on the unit group U_p, of which there is of course only one for any p, whereas for elliptic curves we have the increased flexibility deriving from the numerous elliptic curves over just a single finite field $\mathbb{F}_p$). The second is the generalization of Diffie-Hellman and ElGamal encryption to elliptic curve cryptography ("ECC"), again presented by analogy with the earlier studies. The chapter ends with a discussion of quantum cryptography, in the context of NSA's 2015 policy change promoting quantum-resistant protocols, over its previous preference for ECC. (No details on quantum crypto are given, nor would that be appropriate in light of the mathematical themes of the book.)

Finally, there is an appendix that returns to the motivating problems stated in the beginning, for example the Congruent Number problem, going so far as to state Tunnell's solution, modulo the Birch–Swinnerton-Dyer Conjecture. In addition to presenting enough complex analysis to introduce the L-function associated to an elliptic curve, the Birch–Swinnerton-Dyer Conjecture itself is also outlined. Of course, these are much deeper waters, and the discussion is unavoidably sketchy, but it gives the reader a good sense of what this is about. Finally, there is a brief introduction to elliptic curves over $\mathbb{C}$.

3 Opinion

It should be clear from the above summary that elliptic curves are used here as a medium in which to introduce a rich array of concepts from algebra and number theory, as well as some even more basic principles of mathematical proof, and how mathematics is done. While this part is basic, the author is always mindful of highlighting the deeper ideas and higher truths, which maintains the reader's interest. Furthermore, the style is conversational, much like a teacher discussing the topic with a few students. I know a lot of this stuff, but read it all anyway and never got bored. Seldom does one see such care in mathematical writing addressed

to beginning students.

Indeed, the subtitle "A Beginner's Guide" couldn't be more sincere. The "beginner's" prerequisite for reading this book is, supposedly, a course in calculus. However, its essential requirement is really the mathematical maturity one gets from such a course. It draws on very few specific facts from prior courses. A talented and motivated high school student (willing to accept a few things on faith, as I did) could get a lot out of it. It is by no means a thorough introduction to the subject, but rather gives the reader a taste of it, providing numerous pointers to the literature for in-depth treatments, in many different directions. In that sense, it is truly a "guide," in the same sense that a guided tour of a new city will direct you to all the points of interest that are worthy of further investigation. It is also ideal for self-study, as there are many exercises, most of which are solved in an appendix.

That being said, is there anything here for more advanced students, or even the experienced researcher? Speaking for myself, I knew very little about elliptic curves before reading this book, despite having dipped into a few more advanced texts from time to time to see what it's all about. I now feel like I have a solid perspective on the subject, and much better prepared (and motivated!) to revisit those advanced texts.

It's hard to criticize a book this good, but in the interest of being fair and balanced I'll try anyway. Is there anything categorically wrong with it? Not much. I came across three typos, one on page 179 (an "of" that should have been "or"), one on page 181 (too many "or any"s), and one on page 190 where "later" should be "latter." There are no doubt a few others. I would have liked a more detailed index, e.g., one with entries for "Bachet" and "Bézout," for example, and similarly for other terminology (not only under the B's!) that is introduced early in the book and not referenced until much later. But, to be honest, that's about it. (And to be fair, the author often reminds readers of the meanings of various terms when they reappear.)

In sum, here are the things I liked most about this book. Firstly, everything is driven by examples. You are very unlikely to encounter a definition or theorem that is not accompanied by examples (and non-examples) both before and after it is stated. For example, to illustrate group homomorphisms, we examine the Cayley tables of different groups, and check that they are essentially the same in structure (can't get much more concrete than that!). Secondly, the author *always* explains the "why," not only the "how." *Everything* is cogently motivated. Most importantly, he leads the reader through the *process* of coming up with correct answers, even if that means exploring a few blind alleys, then realizing there are other more promising channels, eventually happening on the "right path." Notably, this strategy is followed in the treatment of projective space and the group law for elliptic curves. The result is a narrative (rather than drily expository) quality that makes for a very reader-friendly experience.

In short, this is a thoroughly enjoyable and elegant book. Highly recommended!