MR2229945 (2007b:11001) 11-01 (11D41 11F80 11G05)

Ash, Avner (1-BSTC); **Gross, Robert** (1-BSTC)

★**Fearless symmetry.**

Exposing the hidden patterns of numbers.

With a foreword by Barry Mazur.

Princeton University Press, *Princeton*, *NJ*, 2006. *xx*+272 *pp*. $24.95.
ISBN 0-691-12492-2; 978-0-691-12492-6

This unique book paints a picture of modern algebraic number theory, culminating in a discussion of Wiles' proof of Fermat's Last Theorem. Inspired by the authors' high-level expository article in [Bull. London Math. Soc. **32** (2000), no. 4, 385–397; MR1760802 (2001h:11142)], the main themes of the book are matrix representations of the absolute Galois group of the rational numbers, and reciprocity laws. Much of what makes the book unique is that the intended audience is expected to know virtually no mathematics beyond calculus, and so the first two-thirds of the book is a friendly introduction to the needed prerequisite concepts. The authors try very hard to avoid the usual "theorem-proof" style, so the book is replete with statements left unproven. As they observe, the book is not written to be a textbook.

The first part, "Algebraic Preliminaries", begins with an insightful discussion of the concept of representation, and follows with chapters on groups, permutations, modular arithmetic, complex numbers, equations and varieties, and quadratic reciprocity. The second part, "Galois Theory and Representations", introduces more advanced topics—the absolute Galois group G of the rational numbers, the Galois group of a polynomial and the restriction morphism, elliptic curves, matrices, matrix groups and group representations and characters. This part concludes with a "working definition" of Frobenius elements at each prime p. To illustrate the engaging style of the book, here is how the authors introduce the Frobenius elements at p in Chapter 16:

"We now begin to define them. If you choose to skip the rest of this discussion, you need to know only:

• Frob_p is a particular element of G.

• Actually, this is a lie, because we cannot define Frob_p so precisely. Really, given p, there is defined a certain conjugacy class in G (depending on p) and Frob_p is taken to be any element in that conjugacy class.

• In fact, we just lied again: Frob_p really is a union of conjugacy classes."

The authors then point out that in subsequent formulas they will only be using the trace of a matrix representation of Frob_p, never Frob_p itself, and then only for "good" primes. But they do compute $\mathrm{Frob}_p(a)$ for $a = i$ and $\sqrt{11}$, and present "an amazing theorem" connecting the cycle type of Frob_p as a permutation on the roots of an irreducible polynomial f over $\mathbb{Z}$ with the factorization of f modulo p. In an appendix to Chapter 16 they present a more precise definition of Frob_p.

The last part of the book, "Reciprocity Laws", introduces the kinds of reciprocity laws they have in mind, namely, the identification of the sequence of traces of the Frobenius matrices for the unramified primes of some representation of G, with a sequence derived "as the output of some

black box", such as the number of solutions modulo primes of certain systems of equations defined over $\mathbb{Z}$, or the Fourier coefficients modulo primes of a modular form. The other well-known "black box", traces of Hecke operators at various primes, the main object of study in the authors' 2000 paper cited above, is viewed as too difficult to present.

The last six chapters elaborate on the reciprocity theme. In Chapter 18 the authors state "an amazing theorem" that given an elliptic curve E over $\mathbb{Z}$, and a prime p, then for any good prime q, the character of Frob_q from the representation of G in $\mathrm{GL}(2, \mathbb{F}_p)$ arising from the p-torsion points of E is congruent to $1 + q - \#E(\mathbb{F}_q)$ modulo p, and they prove it for $p = 2$. In Chapter 19 they interpret the Legendre symbol $(\frac{W}{p})$ as the trace of a one-dimensional representation of Frob_p and describe quadratic reciprocity in that setting. In Chapter 20, "A Machine for Making Galois Representations", they give a very intuitive introduction to étale cohomology groups and the Fontaine-Mazur Conjecture. After asking "What is mathematics?", Chapter 21 discusses the result that every cuspidal normalized newform yields a reciprocity law, and mentions Serre's conjecture about which two-dimensional Galois representations are modular. Chapter 22 introduces the Modularity Conjecture for elliptic curves and connects all these ideas with Wiles' proof of Fermat's Last Theorem. Finally, Chapter 23 recapitulates what the book covered, mentions further related work on generalized Fermat equations and on the congruent number problem, asks "why do math?", and looks into the future.

The focus on reciprocity laws sets this book apart from other expositions of Wiles' proof.

To borrow one of the authors' favorite words, this book is an amazing attempt to provide to a mathematically unsophisticated reader a realistic impression of the immense vitality of this area of mathematics. But I think the book has another useful role. With a very broad brush, it paints a beautiful picture of one of the main themes of the Langlands program. Beginning graduate students could benefit from having this picture in mind as they plunge into the morass of prerequisites needed to work in the field.

Reviewed by *Lindsay N. Childs*