Preface

This book is intended to complement my *Elements of Algebra*, and it is similarly motivated by the problem of solving polynomial equations. However, it is independent of the algebra book, and probably easier. In *Elements of Algebra* we sought *solution by radicals*, and this led to the concepts of *fields* and *groups* and their fusion in the celebrated theory of Galois. In the present book we seek *integer solutions*, and this leads to the concepts of *rings* and *ideals* which merge in the equally celebrated *theory of ideals* due to Kummer and Dedekind.

Solving equations in integers is the central problem of number theory, so this book is truly a number theory book, with most of the results found in standard number theory courses. However, numbers are best understood through their algebraic structure, and the necessary algebraic concepts—rings and ideals—have no better motivation than number theory.

The first nontrivial examples of rings appear in the number theory of Euler and Gauss. The concept of ideal—today as routine in ring theory as the concept of normal subgroup is in group theory—also emerged from number theory, and in quite heroic fashion. Faced with failure of unique prime factorization in the arithmetic of certain generalized "integers", Kummer created in the 1840s a new kind of number to overcome the difficulty. He called them "ideal numbers" because he did not know exactly what they were, though he knew how they behaved. Dedekind in 1871 found that these "ideal numbers" could be realized as *sets* of actual numbers, and he called these sets *ideals*.

Dedekind found that ideals could be defined quite simply; so much so that a student meeting the concept today might wonder what all the fuss is about. It is only in their role as "ideal numbers", where they realize Kummer's impossible dream, that ideals can be appreciated as a genuinely brilliant idea.

Thus solution in integers—like solution by radicals—is a superb setting in which to show algebra at its best. It is the right place to introduce rings and ideals and the right place first to apply them. It even gives an opportunity to introduce some exotic rings, such as the quaternions, which we use to prove Lagrange's theorem that every natural number is the sum of four squares.

The book is based on two short courses (about 20 lectures each) given at Monash University in recent years; one on elementary number theory and one on ring theory with applications to algebraic number theory. Thus the amount of material is suitable for a one-semester course, with some variation possible through omission of the optional starred sections. A slower-paced course could stop at the end of Chapter 9, at which point most of the standard results have been covered, from Euclid's theorem that there are infinitely many primes to quadratic reciprocity.

It should be stressed, however, that this is not meant to be a standard number theory course. I have tried to avoid the ad hoc proofs that once gave number theory a bad name, in favor of unifying ideas that work in many situations. These include algebraic structures but also ideas from elementary number theory, such as the Euclidean algorithm and unique prime factorization. In particular, I use the Euclidean algorithm as a bridge to Conway's visual theory of quadratic forms, which offers a new approach to the Pell equation.

There are exercises at the end of almost every section, so that each new idea or proof receives immediate reinforcement. Some of them focus on specific ideas, while others recapitulate the general line of argument (in easy steps) to prove a similar result. The purpose of each exercise should be clear from the accompanying commentary, so instructors and independent readers alike will be able to find an enjoyable path through the book.

My thanks go to the Monash students who took the courses on which the book is based. Their reactions have helped improve the presentation in many ways. I am particularly grateful to Ley Wilson, who showed that it is possible to master the book by independent study.

Special thanks go to my wife Elaine, who proofread the first version of the book, and to John Miller and Abe Shenitzer, who carefully read the revised version and saved me from many mathematical and stylistic errors.

JOHN STILLWELL
South Melbourne, July 2002

Springer

http://www.springer.com/978-0-387-95587-2

Elements of Number Theory

Stillwell, J.
2003, XII, 256 p., Hardcover
ISBN: 978-0-387-95587-2