Preface

It is widely agreed that Carl Friedrich Gauss's 1801 book *Disquisitiones Arithmeticae* [**G**] was the beginning of modern number theory, the first work on the subject that was systematic and comprehensive rather than a collection of special problems and techniques. The name "number theory" by which the subject is known today was in use at the time—Gauss himself used it (*theoria numerorum*) in Article 56 of the book—but he chose to call it "arithmetic" in his title. He explained in the first paragraph of his Preface that he did not mean arithmetic in the sense of everyday computations with whole numbers but a "higher arithmetic" that comprised "general studies of specific relations among whole numbers."

I too prefer "arithmetic" to "number theory." To me, number theory sounds passive, theoretical, and disconnected from reality. Higher arithmetic sounds active, challenging, and related to everyday reality while aspiring to transcend it.

Although Gauss's explanation of what he means by "higher arithmetic" in his Preface is unclear, a strong indication of what he had in mind comes at the end of his Preface when he mentions the material in his Section 7 on the construction of regular polygons. (In modern terms, Section 7 is the Galois theory of the algebraic equation $x^n - 1 = 0$.) He admits that this material does not truly belong to arithmetic but that "its principles must be drawn from arithmetic."

What he means by arithmetic, I believe, is *exact computation,* close to what Leopold Kronecker later called "general arithmetic."[1]

In 21st century terms, Gauss's subject is "algorithmic mathematics," mathematics in which the emphasis is on algorithms and computations. Instead of set-theoretic abstractions and unrealizable constructions, such mathematics deals with specific operations that arrive at concrete answers. Regardless of what Gauss might have meant by his title *Disquisitiones Arithmeticae,* what I mean by my title *Higher Arithmetic* is an algorithmic approach to the number-theoretic topics in the book, most of which are drawn from Gauss's great work.

Mathematics is about reasoning, both inductive and deductive. Computations are simply very articulate deductive arguments. The best theoretical mathematics is an inductive process by which such arguments are found, organized, motivated, and explained. That is why I think ample computational experience is indispensable to mathematical education.

In teaching the number theory course at New York University several times in recent years, I have found that students enjoy and feel they profit from doing computational assignments. My own experience in reading Gauss has usually been that I don't understand what he is doing until he gives an example, so I try to skip to the example right away. Moreover, on another level, in writing this and previous books, I have often found that creating exercises leads to a clearer understanding of the material and a much improved version of the text that the exercises had been meant to illustrate. (Very often, the greatest enlightenment came when writing *answers* to the exercises. For this reason, among others, answers are given for most of the exercises, beginning on page 179.)

Fortunately, number theory is an ideal subject from the point of view of providing illustrative examples of all orders of difficulty. In this age of computers, students can tackle problems with real computational substance without having to do a lot of tedious work. I

[1] See Essay 1.1 of my book [**E3**]. For the relation of general arithmetic to Galois theory, see Essay 2.1.

have tried to provide at the end of each chapter enough examples and experiments for students to try, but I'm sure that enterprising students and teachers will be able to invent many more.

What began as an experiment in the NYU course turned into a substantial revision of the course. The experiment was to see how much of number theory could be formulated in terms of "numbers" in the most primitive sense—the numbers 0, 1, 2, ... used in counting. To my surprise, I found that not only could I *avoid* negative numbers but that I *didn't miss* them. The simple reason for this is that the basic questions of number theory can be stated in terms of congruences, and subtraction is always possible in congruences without any need for negative numbers. Negative numbers have always led to metaphysical conundrums—why should a negative times a negative be a positive?—which cause confusing distractions right at the outset when the meaning of "number" is being made precise. In this book, the meaning of "number" derives simply from the activity of counting and arithmetic can begin immediately. Kronecker's famous dictum, "God created the whole numbers; all the rest is human work," can be amended to say, "nonnegative whole numbers," which is very likely what Kronecker meant anyway.

A central theme of the book is the problem I denote by the equation $A\Box + B = \Box$, the problem of finding, for two given numbers A and B, all numbers x for which $Ax^2 + B$ is a square. As Chapter 2 explains, versions of this problem are at least as old as Pythagoras, although two millennia later the *Disquisitiones Arithmeticae* still dealt with it. A simple algorithm for the complete solution is given in Chapter 19.

Work on problems of the form $A\Box + B = \Box$ led Leonhard Euler to the discovery of what I call "Euler's law," the statement that the answer to the question "Is A a square mod p?" for a prime number p depends only on the value of p mod $4A$. This statement, of which the law of quadratic reciprocity is a byproduct, is completely proved in Chapter 29.

When Ernst Eduard Kummer first introduced his theory of "ideal complex numbers" in 1846, 45 years after the publication of *Disquisitiones Arithmeticae,* Gauss said that he had worked out something

resembling Kummer's theory for his "private use" when he was writing about the composition of binary quadratic forms in Section 5 of *Disquisitiones Arithmeticae,* but that he left it out of the book because he had not been able to put it on firm ground.[2] Although the proof of quadratic reciprocity given in this book was originally inspired by Gauss's proof using the composition of forms, it is stated in terms closer to Kummer's ideal numbers. Specifically:

If, in addition to using ordinary numbers 0, 1, 2, ... , one computes with a symbol $\sqrt{A}$ whose square is a fixed number A, one has an arithmetic—I have dubbed it the arithmetic of "hypernumbers" for that A—in which the natural generalization of doing computations mod n for some number n is to do computations mod $[a, b]$ for some *pair* of hypernumbers a and b. (With ordinary numbers, the Euclidean algorithm serves to reduce the number of numbers in a set that describes a modulus to just one, but with hypernumbers two may be needed, as is shown in Chapter 18.) With natural definitions of multiplication and equivalence of such "modules of hypernumbers," the computations needed to solve $A\Box + B = \Box$ and to prove quadratic reciprocity can be explained very simply. In this way, Gauss's difficult composition of forms is avoided but the essence of his method is preserved.

The last two chapters relate the methods of the book to Gauss's binary quadratic forms so students interested in reading further in the *Disquisitiones Arithmeticae*—or students interested in binary quadratic forms—will be able to make the transition.

Finally, an appendix gives a table of the cycles of stable modules of hypernumbers for all numbers $A \leq 111$ that are not squares, which will be useful for students, as they were for me, in understanding the general theory and in working out examples.

[2]See [**E4**].