Preface

This book is about a major breakthrough in an important part of number theory and how algebraic curves play a central role in this revolution. Many problems that once posed a challenge for experienced mathematicians have become virtually routine to solve. This book is an informal and leisurely introduction to understanding this revolution and how to apply its methods to solve a large class of what are called "Diophantine equations." In general, solving such equations means finding integer solutions to polynomial equations with integer coefficients. In many of the most important cases, the polynomial terms all have the same degree, and then we can apply a powerful method that works like a blowtorch: Translate the problem to one in geometry where intuition is a potent aid and solve it there. Then translate back to the world of integers to see the final solution.

Our approach is concrete with lots of pictures and solved numeric problems. The power and simplicity of the new method makes a large swath of formerly difficult problems easy to solve. In fact, you'll be able to devise nontrivial number theory problems on your own and solve them using the method.

The background needed for the early chapters of this book is mainly high school math. Some familiarity with Mathematica and Maple will be helpful, and for those wishing to use freeware, GeoGebra fills the bill admirably. Using any of these powerful tools requires some coding, and Appendix C supplies code or pseudocode for those wanting it. In the last half of the book we encounter some basic concepts covered in a typical undergraduate math major, mostly from beginning group theory and linear algebra. The book also includes sketches of some enlightening theory. To read these parts, a basic course in complex variables and one in topology should suffice.

A little Q&A between writer and potential reader will help elucidate the overall design of the book:

- *What kind of number theory problems are we talking about?* They are problems in three integer unknowns. For example, find all integer solutions to

$$a^2 + b^2 = c^2$$

or to

$$3a^2 - 5c^2 = 11b^2$$

or to really crazy ones like

$$-91b^2 + 37c^2 + 84a^2 = 0\,.$$

You, or a computer, could doubtless find some specific solutions, *but finding all of them?* It turns out that either there are no solutions at all or an infinite number of them. The approach helps you decide which is which, and in the infinite case, the method provides a way of finding them all.

- *What kind of geometry are we talking about?* We're talking about curves defined by an equation $p(x, y) = 0$, where $p(x, y)$ is a polynomial having integer coefficients and degree ≤ 3. That means lines, circles, ellipses, parabolas, hyperbolas, and a wide variety of cubic curves.

- *What do we do with these curves?* We drain away most of the points in the plane, leaving only those having rational numbers for both coordinates. What's left of the curve constitutes precisely the geometric version of all solutions to the problem. We then translate back to the world of integers. (A quick aside: A rational number is any number that can be written as a fraction or ratio of integers such as $\frac{2}{1}$ or $\frac{5}{10}$. The nonfractions 2 and 0.5 are rational numbers since they can be rewritten as fractions. Notice that "rational" contains the word "ratio.")

- *But how do we translate to geometry?* We divide the equation through by a power of a, b, or c to get rid of it. For example, divide $a^2 + b^2 = c^2$ by c^2 to get $x^2 + y^2 = 1$, where x and y are the rational numbers $\frac{a}{c}$ and $\frac{b}{c}$. It's $x^2 + y^2 = 1$ that defines our curve — in this case, a circle. After draining away all the nonrational points, we're staring at *the geometric solutions to the problem.*

- *Impressive, but how do we actually get specific solutions? And from what you said, there must be an infinite number of them!* Still looking at $a^2+b^2 = c^2$ as a representative example, pick a point such as $(-1, 0)$ on the corresponding circle $x^2 + y^2 = 1$. Through this point, pass a line having rational slope and solve for the other point where the line meets the circle. This involves only high school math, but it's powerful. Just make up any rational number you want for the slope, and you get another solution. As we'll see in the book, the rational number $\frac{1}{2}$ gives $\left(\frac{3}{5}, \frac{4}{5}\right)$. To get integers, just multiply $\left(\frac{3}{5}, \frac{4}{5}\right)$ through by the denominator. For example,

$$\left(\frac{3}{5}\right)^2 + \left(\frac{4}{5}\right)^2 = 1$$

becomes

$$3^2 + 4^2 = 5^2 .$$

So $\frac{1}{2}$ gives the famous right triangle $(3, 4, 5)$. You can make up fancier rationals and get corresponding right triangles. For example, $\frac{7}{5}$ gives the right triangle $(24, 70, 74)$ — a more unusual example.

- *So you just multiply through to change rational numbers into integers? That's how you translate from geometry to number theory?* That's it. The only restriction on the original a, b, c problem is that when you translate to a curve, you get a polynomial $p(x, y)$ whose locus is a curve. That means when you divide by, say, c^2 in $a^2 + b^2 = c^2$, there is no c left over after writing $x = \frac{a}{c}$ and $y = \frac{b}{c}$. That always works provided the terms involving a, b, c all have the same degree. We call such an equation "homogeneous." That's true of all the examples mentioned above, but it wouldn't be true for something like $a^2 + b^2 = c$, for example. So in fancier language, this book is about

$$\boxed{\text{solving homogeneous Diophantine equations of degree} \leq 3.}$$

- *So you get every possible integer solution using this method?* Very close to that! Here's how to get all solutions to any degree-two homogeneous Diophantine equation in integer variables a, b, c: Let m run through the values $\mathbb{Q} \cup \{\infty\}$ and for each such value, find a "primitive" solution — a triple of integers (a, b, c) where a, b, c have no common factors other than ± 1. If the triple you have isn't primitive, you can make it so by dividing the triple through by the greatest common divisor of (a, b, c). Then up to sign, any solution to the homogeneous Diophantine equation is obtained by multiplying that primitive solution by some integer to get (an, bn, cn). For the problem $a^2 + b^2 = c^2$, for example, the slope $\frac{1}{2}$ leads to $(3, 4, 5)$ which is primitive, so up to signs, every solution corresponding to $\frac{1}{2}$ is

$$(\pm 3n, \pm 4n, \pm 5n) \ \ (n \in \mathbb{Z}),$$

where the ± are taken independently from coordinate to coordinate. And that slightly strange case of slope $\frac{7}{5}$? It led to $(24, 70, 74)$. This triple has 2 as a common factor, so $(12, 35, 37)$ is primitive, and every solution of $a^2 + b^2 = c^2$ corresponding to that slope is

$$(\pm 12n, \pm 35n, \pm 37n) \ \ (n \in \mathbb{Z}).$$

I want to express my great gratitude to those who have helped make this book a reality. Its original inspiration and much of its content came from Manjul Bhargava's beautiful Hedrick Lectures on this subject given during the Mathematical Association of America's summer meeting in 2011. It is my pleasure to dedicate this book to him. (See the biographical sketch about him on pp. 130–135.) I am also greatly indebted to Don Albers, past Acquisitions Editor of the MAA, who was both constant cheerleader and wise counsel in writing this book. Stephen Kennedy took over after Don's retirement and has likewise given me much helpful advice. Special thanks are due Harriet Pollatsek, Editor of the Dolciani Series, as well as her successor Ray Rosentrater. The entire Dolciani Board, appearing on p. iv, has been a model of thoroughness; the book has been significantly improved, thanks to their conscientious work. I would also like to express appreciation in a slightly different direction. Just as a concert pianist owes a debt of gratitude to the years of work and ingenuity that went into the many improvements resulting in a magnificent instrument, I too owe a debt of gratitude to the designers of the powerful and reliable software that became my constant companions as I wrote this book. At the top of the list has to be PCTeX used in writing the text. As for the figures, Adobe's Illustrator and Photoshop were indispensable to me. On the mathematical side of the ledger, Maple, Mathematica, and GeoAlgebra were all a great help. Kudos to the many talented developers of such beautiful software!

Keith Kendig
Chagrin Falls, OH
March 2021