Franz Lemmermeyer

Pell Conics

An Alternative Approach to Elementary Number Theory

November 30, 2012

Franz Lemmermeyer
Jagstzell, Germany

Preface

These days, there are many textbooks introducing readers with varying backgrounds to elementary number theory, and there seems to be a choice for everyone's taste. It obviously does not make any sense to add yet another book to this almost endless list unless the approach differs substantially from those adopted by other books.

Being original in a time-honoured subject such as number theory is not an easy task. It goes without saying that a textbook, like any set of lecture notes that can be found all over the world wide web, must include the standard results and the basic methods of proof. But just as a house is more than a collection of rooms, a good number theory text is more than a collection of definitions, theorems and proofs: it should convey the author's love for a particular subject, it should present motivation[1], emphasize important insights, and should contain a few surprises.

In this book I aim at presenting number theory as an attempt at understanding zeta functions; as we will see, not only the obvious candidates such as various prime number theorems are deeply connected with properties of zeta functions, but so are unique factorization (via the Euler product) and quadratic reciprocity (via modularity). The zeta functions that we will study here are tied to objects called Pell conics: these are rational curves described by the Pell equation.

The choice of basing a whole course on the Pell equation $x^2 - my^2 = 1$ seems to have one big advantage over the more traditional approaches: almost everything we do here can also be done for elliptic curves, objects that have become of central importance both in the teaching of number theory as well as in research and cryptographical applications. By studying the arithmetic of conics we not only give a well motivated introduction to the main topics of a course in elementary number theory (unique factorization, congruences, residue class rings, quadratic reciprocity): we prepare the readers at the same time for the more advanced concepts they may or may not see later, such as congruence zeta functions, analytic methods, or modularity.

There are two number theory books I know of that also put the Pell Equation in the center: "The Pell Equation" by Ed Barbeau is a very nice book on a more elementary level; "Solving the Pell Equation" by Jacobson and Hugh Williams is more research oriented. Neither of them is a textbook in elementary number theory in the sense that it covers the standard material, and the intersection with the present book is in both cases rather small.

The usual content of an introduction to elementary numbers theory is presented in Part I and includes the theory of congruences and unique factorization (Chap. 1), and the structure of residue class rings (Chap. 3). In Chap. 2 we present a couple of Pell conics and study some of their more elementary properties; in Chap. 4 we transfer the results on residue classes obtained in Chap. 3 to general conics.

[1] There are only a few books can do without motivational material – I am thinking in particular of Landau's great books on elementary, algebraic and analytic number theory, all of which can be read with profit today.

Part II is devoted to applications of our results to to algorithmic number theory and cryptography. In Chap. 5) we will discuss primality tests, primality proofs, and some basic factorization methods, as well as a quick way of computing square roots modulo prime numbers. In Chap. 6 we discuss a few applications of elementary number theory and Pell conics to cryptography.

The more advanced parts of the arithmetic of Pell conics begins with Part III. There we will deal with quadratic reciprocity, which we introduce as a modularity property of Pell conics in Chap. 7. This leads immediately into the theory of quadratic Gauss sums; it is also connected with several simple analytic questions concerning the Riemann zeta function and Dirichlet series, which we will treat in Chap. 8 and Chap. 9.

The final Part IV presents a first introduction to the theory of descent on Pell conics. In Chapter 10 we imitate the theory of 2-descent on elliptic curves in the case of conics and show that the group of integral (or, more generally, of S-integral) points on a Pell conic $\mathcal{C}$ is finitely generated. In subsequent chapters we then deal with the solvability of the Pell equation and cyclotomic unit varieties.

Each chapter contains, in addition to the usual definitions, theorems and proofs, a set of historical notes. In these notes, the usual suspects (Fermat, Euler, Gauss) could not be avoided, nor was I trying to. I did attempt, however, to provide information on little known mathematicians who have contributed one way or another to our knowledge, and whose work often either was not noticed at all or was instantly forgotten.

In addition to lemmas, propositions and theorems I have used statements called "Facts" which merely are "clarifications" of a definition. Proofs of "facts" are usually left to the reader and are usually "formal" in the sense that they require nothing beyond the definition of certain objects.

The prerequisites for reading this book are modest: for most parts, a familiarity with the basic structures of algebra (such as groups, rings and fields) and linear algebra (vector spaces) will be more than enough. Readers who have not yet been exposed to these abstract concepts will find the necessary definitions scattered throughout the text (except for the notions of a field and a vector space, which I assume is known from introductions to linear algebra). Some sections also use elementary calculus (convergence of series, power series, even differential equations).

The arithmetic of conics is far from being exhausted by the material presented here. I have plans for sequels in which I will explain the algebra and the geometry of Pell conics, as well as the classical theory of binary quadratic forms together with an elementary introduction to the arithmetic of elliptic and hyperelliptic curves. These volumes will also contain results that I was forced to omit here, and which will make the analogy between Pell conics and elliptic curves even more visible.

Among the tools I have used I would like to mention in particular LaTeX (of course) for writing this book, `pari` and `sage` for doing calculations, and `geogebra` for drawing most of the pictures. All of these programs are freeware, thanks to the efforts of the many people who have contributed their time and their energy to developing these tools.

It is a great pleasure for me to thank Soun-Hi Kwon for inviting me to Seoul in 2002, where the whole idea with descent on Pell conics first developed as a toy example for explaining the arithmetic of elliptic curves. I enjoyed a long email discussion in 2003 with Jeff Lagarias on various aspects of descent on Pell conics. Finally, Samuel Hambleton contributed significantly to the theory of Pell conics with his own work, and in particular found the elementary proof that the Weil map is a homomorphism.

Contents