This book can be divided into two parts. The first part is preliminary and consists of algebraic number theory and the theory of semisimple algebras. The raison d’être of the book is in the second part, and so let us first explain the contents of the second part.

There are two principal topics:

(A) Classification of quadratic forms;
(B) Quadratic Diophantine equations.

Topic (A) can be further divided into two types of theories:

(a1) Classification over an algebraic number field;
(a2) Classification over the ring of algebraic integers.

To classify a quadratic form \( \varphi \) over an algebraic number field \( F \), almost all previous authors followed the methods of Helmut Hasse. Namely, one first takes \( \varphi \) in the diagonal form and associates an invariant to it at each prime spot of \( F \), using the diagonal entries. A superior method was introduced by Martin Eichler in 1952, but strangely it was almost completely ignored, until I resurrected it in one of my recent papers. We associate an invariant to \( \varphi \) at each prime spot, which is the same as Eichler’s, but we define it in a different and more direct way, using Clifford algebras. In Sections 27 and 28 we give an exposition of this theory. At some point we need the Hasse norm theorem for a quadratic extension of a number field, which is included in class field theory. We prove it when the base field is the rational number field to make the book self-contained in that case.

The advantage of our method is that it enables us to discuss (a2) in a clear-cut way. The main problem is to determine the genera of quadratic forms with integer coefficients that have given local invariants. A quadratic form of \( n \) variables with integer coefficients can be given in the form \( \varphi[x] = \sum_{i,j=1}^n c_{ij} x_i x_j \) with a symmetric matrix \((c_{ij})\) such that \( c_{ii} \) and \( 2c_{ij} \) are integers for every
If the matrix represents a symmetric form with integer coefficients, then $c_{ij}$ is an integer for every $(i, j)$. Thus there are two types of classification theories over the ring of integers: one for quadratic forms and the other for symmetric forms. In fact, the former is easier than the latter. There were several previous results in the unimodular case, but there were few, if any, investigations in the general case. We will determine the genera of quadratic or symmetric forms over the integers that are reduced in the sense that they cannot be represented by other quadratic or symmetric forms nontrivially. This class of forms contains forms with square-free discriminant.

We devote Section 32 to strong approximation in an indefinite orthogonal group of more than two variables, and as applications we determine the classes instead of the genera of indefinite reduced forms.

The origin of Topic (a2) is the investigation of Gauss concerning primitive representations of an integer as a sum of three squares. In our book of 2004 we gave a framework in which we could discuss similar problems for an arbitrary quadratic form of more than two variables over the integers. In Chapter VII we present an easier and more accessible version of the theory. Though Gauss treated sums of three squares, he did not state any general principle; he merely explained the technique by which he could solve his problems. In fact, we state results as two types of formulas for a quadratic form, which can be specialized in two different ways to what Gauss was doing. Without going into details here we refer the reader to Section 34 in which a historical perspective is given. Our first main theorem of quadratic Diophantine equations is given in Section 35, from which we derive the two formulas in Section 37.

Let us now come to the first part of the book in which we give preliminaries that are necessary for the main part concerning quadratic forms. Assuming that the reader is familiar with basic algebra, we develop algebraic number theory and also the theory of semisimple algebras more or less in standard ways, and even in old-fashioned ways, whenever we think that is the easiest and most suitable for beginners. In fact, almost all of the material in this part have been taken from the notes of my lectures at Princeton University. However, we have tried a few new approaches and included some theorems that cannot be found in ordinary textbooks. For instance, our formulation and proof of the quadratic reciprocity law in a generalized form do not seem to be well-known; the same may be said about the last theorem of Section 10, which is essentially strong approximation in a special linear group. In the same spirit, we add the classical theory of genera as the last section of the book.

We could have made the whole book self-contained by including an easy part of class field theory, but in order to keep the book a reasonable length,
we chose a compromised plan. Namely, we prove basic theorems in local class
field theory only in some special cases, and the Hilbert reciprocity law only
over the rational number field. However, we at least state the main theorems
with an arbitrary number field as the base field, so that the reader who knows
class field theory can learn the arithmetic theory of quadratic forms with no
further references.

To conclude the preface, it is my great pleasure to express my deepest
thanks to my friends Koji Doi, Tomokazu Kashio, Kaoru Okada, and Hiroyuki
Yoshida, who kindly read earlier versions of the first two-thirds of the book
and contributed many invaluable comments.

Princeton
May, 2009

Goro Shimura
Arithmetic of Quadratic Forms
Shimura, G.
2010, XII, 238 p., Hardcover
ISBN: 978-1-4419-1731-7