[Sch] W. Schmid, *Boundary value problems for group invariant differential equations*, Astérisque, Elie Cartan et les Mathematiques d'aujourd'hui, 1983.

[Wa] N. Wallach, *Asymptotic expansions of generalized matrix entries of representations of real reductive groups*, Representations of Lie groups I, Lecture Notes in Math., vol. 1024, Springer-Verlag, Berlin, 1983, pp. 287–369.

[We] H. Weyl, *Uber gewohnliche Differentialgleichungen mit Singularitaten und die zugehorigen Entwicklungen willkurlicher Funktionen*, Math. Ann. **68** (1910), 220–269.

D. Barbasch
Rutgers University

BULLETIN (New Series) OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 23, Number 2, October 1990

0273-0979/90 $1.00 + $.25 per page

Binary quadratic forms, classical theory and applications, by D. A. Buell. Springer-Verlag, New York, Berlin, 1989, 247 pp., $35.00.

As the subtitle indicates, this book was written with the intention of alerting the computer-minded reader to the possibility of applying some part of the theory of binary quadratic forms to various problems.

In 1801 Gauss laid the foundation of the arithmetic of the forms $f(x, y) = ax^2+2bxy+cy^2$ in sections 153–335 of the *Disquitiones Arithmeticae.* By 1850 the theory of algebraic numbers, the theory of ideals and the theory of class groups were beginning to emerge. This forced the rewriting of Gauss theory using the Eisenstein form $f(x, y) = ax^2 + bxy + cy^2 = (a, b, c)$, with the discriminant $\Delta = b^2 = 4ac$. This revised Gauss theory is what the author describes as the classical theory.

On page 2, three questions are proposed:

(a) What integers can be represented by a given form?
(b) What forms can represent a given integer?
(c) If a form represents an integer, how many representations exist and how may they all be found?

These questions are answered on pages 74–75 by six theorems. The reader is thus required to read four chapters, whose titles are Elementary Concepts, Reduction of Positive Definite Forms, Indefinite Forms, and The Class Group, to prove these theorems.

If the invariant Δ is negative, then

$$ax^2 + bxy + cy^2 = m \tag{1}$$

is the equation of an ellipse and so has only a finite number of lattice points on it. If $|b| \leq a \leq c$, the form (a, b, c) is called reduced. If, on the other hand, Δ is positive, then (1) is the equation of a hyperbola and has an infinite number of lattice points on it. If $0 < b < \Delta^{1/2}$ and $\Delta^{1/2} - b < 2|a| < \Delta^{1/2} + b$, then the form (a, b, c) is called reduced.

The next several chapters deal with the number of equivalence classes of forms of discriminant Δ, the class group formed under composition, generic characters of this group and quadratic fields and their ideals. Needless to say, these topics are all interrelated.

The last chapter is entitled Factoring with Quadratic Forms. The author discusses, along with classical methods beginning with Fermat, four different methods of factoring due to Shanks and dating from 1969. These are denoted by SQUFOF, CLASNO, SPAR and CPRAC. These algorithms are discussed informally and some comparisons of them are made.

There are four little tables on pages 224–243 giving the list of discriminants Δ and their class numbers for $|\Delta| \leq 10,000$. Only squarefree values of Δ are given because there is a formula connecting $h(\Delta p^2)$ with $h(\Delta)$. More specifically, the first two tables are for odd and even $\Delta < 0$, and give h/g and g, where g is the number of genera of Δ and is a power of 2. The last two tables for $\Delta > 0$ give the class number $h(\Delta)$ and a plus or minus sign which corresponds to the Pell equation $x^2 - Dy^2 = \pm 4$, from which the number of classes was deduced. These tables are for the reader's benefit and were taken from the author's tapes of data running into the millions.

There is a bibliography of some 120 items. A curious typographical error occurs at the bottom of page 191, where Fermat is cut off in a quotation. In a second printing, a line of type should be added at this place.

The book should be in demand among those computer professionals who want to learn about binary quadratic forms and their applications.

D. H. LEHMER
UNIVERSITY OF CALIFORNIA, BERKELEY