or anonymous ftp. The exposition benefits from the author's decision to sacrifice some generality when simpler arguments are available. Pointers to an extensive bibliography provide additional details. Many "difficult" topics such as stopping criteria and implementation issues are discussed, and the experimental comparisons running through the book are useful. As a text it will probably need to be supplemented, especially for linear systems. (For example, there is nothing about symmetric indefinite linear systems.) I downloaded and ran one example of the software (GMRES) and found it easy to use as well as to modify.

The one flaw in the book concerns its editing. I noticed enough typographical and grammatical errors to prompt me to start keeping a running count; I observed ten such errors in one thirty-three page interval. Otherwise, the book is well-written and I believe well-suited as an introduction to this material.

HOWARD ELMAN

11[11R11, 11R29, 11Y40]—*Quadratics*, by Richard A Mollin, The CRC Press Series on Discrete Mathematics and Its Applications, CRC Press, Boca Raton, FL, 1966, xx + 387 pp., 26 cm, $74.95

The title refers to any and all aspects of quadratic fields. The author has written a large number of papers (many in collaboration with H. C. Williams) and this book serves very well as a platform for related topics. The most obvious purpose fulfilled by this book (and by none other at present) is the large bibliography with references of hundreds of papers, incidental or central to quadratic fields.

The book tends to accept the classical theory as a necessary evil in order to present the exotica, and indeed this book is not meant for the unacquainted to learn about quadratic fields. Nevertheless, a reader with only a casual acquaintance with quadratic fields will find very many rewarding byways. For this reader, the book is best appreciated at first contact by browsing all the way from beginning to end, and then going back. The review is written in this spirit, with a somewhat arbitrary choice of topics.

[The reviewer's reference to "exotica" among the contents is not necessarily negative. At one time, e.g., nonunique factorization was more or less in this category, yet it became the primary challenge of "main line" Number Theory.]

The author favors the ideal-theoretic approach very strongly but the reader should also understand that there is a case for quadratic forms which is characteristically *quadratic* rather than a special case of fields of arbitrary degree:

The composition of quadratic forms. *The theory of (binary) Quadratic Forms is nothing but the study of the (Gauss) composition identity*

$$(a_1x_1^2 + bx_1y_1 + a_2cy_1^2)(a_2x_2^2 + bx_2y_2 + a_1cy_2^2) = (a_1a_2x_3^2 + bx_3y_3 + cy_3^2),$$

with variables satisfying a bilinear relation over $\mathbb{Z}[a_1, a_2, b, c]$, *namely*

$$x_3 = x_1x_2 - cy_1y_2, \qquad y_3 = a_1x_1y_2 + a_2x_2y_1 + by_1y_2.$$

This identity involves three quadratic forms of discriminant $d = b^2 - 4a_1a_2c$, and the relation to algebraic number theory comes from the norm "N" in

$$ax^2 + bxy + cy^2 = N(ax + (b + \sqrt{d})y/2)/a, \ (d = b^2 - 4ac).$$

So the forms are associated with the modules like $\{ax + (b + \sqrt{d})y/2 : x, y \in \mathbf{Z}\}$. Ideal theory enters in a natural way and is a tool for easy generalization to fields of arbitrary degree, once the bilinear concept is utilized.

One step beyond the composition identity, the object is to represent a number by a quadratic form, and the identity shows that if the prime factors are represented by forms, the factors can be put together to represent the number by multiplying forms. Forms under unimodular equivalence represent the same numbers, so this equivalence class concept is natural. Under the equivalence class concept, any two forms of the same discriminant have equivalent forms satisfying such an identity (possibly with minor restrictions in case $\gcd(a_1 a_2, d) \neq 1$).

For Gauss this was a system which circumvents nonunique factorization. For instance, in the classic case $\mathbf{Q}(\sqrt{-5})$ there are two factorizations of 9 manifesting nonuniqueness,

$$3 \cdot 3 = (2 + \sqrt{-5}) \cdot (2 - \sqrt{-5}).$$

These factorizations correspond to two inequivalent forms with $d = -20$,

$$\Phi_1(x, y) = (x^2 + 5y^2), \qquad \Phi_2(x, y) = (2x^2 + 2xy + 3y^2),$$

(inequivalent since $\Phi_1(1, 0) = 1$, but $\Phi_2(x, y) \neq 1$ for all $x, y \in \mathbf{Z}$.) The equivalence classes form a group of two elements: $\Phi_2^2 = \Phi_1$, viz.,

$$\Phi_2(x, y) \cdot \Phi_2(x - y, y) = \Phi_1(2x^2 + 2y^2, y^2).$$

From here, the theory goes to the multiplication of modules and finally to ideal class structure. This is the classical motivation for "quadratics".

The author, reversing history, develops ideals and makes quadratic forms just an appendix item. In terms of parameters and coordinates, the modules are more useful as a concrete practical model for the forms.

Of course, this does not mean the book is insensitive to history. To the contrary, there is a parallel commentary in footnotes and text which is very engaging and is worth reading, even for experts. In some places, the footnotes on main line history are in contention with the text. Anyway, the author is in the game for exotica, much of which is in topics featuring his own research and that of his students.

In each chapter, after he disposes of theory (sometimes very quickly) he gets down to business. The exercises are very helpful as they serve as an excellent (and necessary) method of understanding the proofs and his favorite techniques.

In Chapter I (Algebraic Number Theory), "powerful" numbers seem to come at us out of nowhere. These are numbers of the form $n = x^2 y^3$ (alternatively $p \mid n \Rightarrow p^2 \mid n$). The first interesting theorem on them is that for every $(0 \neq) m \in \mathbf{Z}$, the diophantine equation $x^2 y^3 - u^2 v^3 = m$ is solvable infinitely often. If $m (= 2t+1)$ is odd, then trivially $m = (t+1)^2 - t^2$, but the *infinitude* is not trivial. The author's clever trick is to devise $Ar^2 - Bs^2 = m$ and then to solve $T^2 - rsU^2 = \pm 1$. Then an infinitude of exponents k are found (in a Fermat-type congruence class) such that

$$(A\sqrt{r} + B\sqrt{s})(T + U\sqrt{rs})^k = gr\sqrt{r} + hs\sqrt{s}.$$

The norm operation completes the proof. This method leads to nine special cases with A, B, r, s, T, U parametrized by m and k. The author then proceeds to a plethora of theorems, lemmas, and conjectures. The effect seems a "bit much", but it is somewhat justified by the apparent connection of the above equation with the conjecture of Ankeny, Artin, Chowla and of Mordell that the coefficient of $\sqrt{p}$ in the fundamental unit for $\mathbf{Q}(\sqrt{p})$ is not divisible by p (prime). The conjectures have

a role in class field theory (which is usually considered to be main line rather than exotic).

Chapter II (on Continued Fractions) is set up in great detail as one of the author's main tools; the complex case is included. Cases of short period for $\mathbf{Q}(\sqrt{D})$, $D = s^2 + r$, $r \mid 4s$, (called "ERD" for "Extended Richaud-Degert") are enumerated in detail in Chapter III (Diophantine Equations and Class Number), and are tools which do not have long to wait for use as illustrations with which we *can actually calculate*. The exercises also cover other more classical exercises such as Lucas-Lehmer Theory and the equation $x^2 - D = p^n$ for fixed $D < 0$ and p prime. (The continued fractions of the basis of a real quadratic field were given the attractive name, "the Infrastructure" by Shanks.)

Here we come to a serious bit of exotica, due to Weinberger and Yamamoto. Let a be odd and let $D = a^{2n} + 4$ be primitive (i.e., D/g^2 is not a discriminant for any $g > 1$). Then $\mathbf{Q}(\sqrt{D})$ has class number divisible by n. (Indeed, the divisors of a have order divisible by n.) There are also infinitely many such D so *there is an (explicit) infinitude of quadratic fields of class number divisible by any given* n. This is an illustration of the frequent trick of using the ERD type of radicand $D = s^2 + 4$.

Chapter IV (Prime-Producing Polynomials) and Chapter V (Class Numbers: Criteria and Bounds) produce the main chain of connected results. The Euler-Rabinowitsch polynomials are

$$f(x) = x^2 + x + m, \qquad m \in \{1, 2, 3, 5, 11, 17, 41\},$$

with the property that $f(x)$ is prime for $x = 0, \ldots, m - 2$ (vacuously true for $m = 1$). The inference that $\mathbf{Q}(\sqrt{1 - 4m})$ has class number one is an exciting result, particularly since the connection with class number works both ways. Ultimately, similar (prime-producing) polynomials come at us en masse (again diluting the excitement of the original polynomials), but leading to criteria of class number one and bounds on the class number. These bounds acquire a special urgency from Gauss's conjecture that for real quadratic fields, the class number may equal one for infinitely many (prime) discriminants.

The most prolific bounds come from the GRH (Generalized Riemann Hypothesis) on the zeros of L-functions as well as ζ-functions. Here, not unexpectedly by now, a lemma (of Tatuzawa) comes out of nowhere, giving

$$L(1, \chi) > .655\varepsilon D^{-\varepsilon},$$

for $.5 > \varepsilon > 0$ and $D > \max\{e^{1/\varepsilon}, e^{11.2}\}$, with D the fundamental discriminant for the L-function. This in turn creates an easy lower bound on the class number, which has $L(1, \chi)$ as a factor in the famous Dirichlet formula.

It would be enlightening to most readers to show even by sketchy heuristics how this inequality is related to the GRH, but the author is too intent on applying this bound, and apply it he does. We have a set of interlocking conjectures of Yokoi, Mollin, and Williams which succeed in establishing that if we restrict our discussion to the (more tractable) ERD-cases, then for discriminant > 1757 the class number exceeds one (unless one exceptional discriminant comes from the failure of the GRH).

Chapter VI (Ambiguous Ideals) deals with ambiguous (self-conjugate) ideals and ideal classes. The problem is usually restricted by starting from equivalent quadratic forms. The author approaches it in full generality, using his method

of palindromic continued fractions. There are applications to statements of when the class group is a 2-group. Chapter VII (Infrastructure) discusses a concept of Shanks, namely the "quadratic residue cover" for a function, i.e., a finite set of primes such that every value of the function is divisible by or is a residue of one of the primes. If the function is a sequence of discriminants, there is ready-made information on nonprincipal ideals, which relates to the class number.

Chapter VIII (Algorithms) is a nonidiosyncratic discussion of factorization and primality. The final section of the text, however, on Computation, is a thoughtful commentary, (basically accepting computers as a fact of life). It also almost reads like a personal testament of the author, but for that matter so does the whole book.

This book is followed by an appendix of 85 pages of numerous tables for units and class numbers, etc. There are also commendably dozens of tables in the text illustrating many of the theorems. These show the author's intense desire to inspire experimentation and reader participation.

Yet mathematics books also have browsers, who want to open a book and come up with a result (maybe also with a proof), just the way a brewery has visitors who do not want to buy the brewery, but just want to enjoy a free beer. The author does not make it easy for such casual readers. Most results have some nonstandard symbol, abbreviation, or neologism which requires further cross-references by the reader, perhaps causing the uncommitted reader's curiosity to wane.

The classical style once required that the more important the theorem the fewer the symbols and plainer the prose. The reviewer wishes the author were more so inclined, but the book is still well worth the effort (and the extra effort).

HARVEY COHN
IDA-CCS
17100 SCIENCE DRIVE
BOWIE, MD 20715-4300
E-mail address: hcohn@super.org

12[11A41, 11-04, 11N36, 11Y60, 68M15]—*Enumeration to* 10^{14} *of the twin primes and Brun's constant*, by Thomas R. Nicely, Virginia Journal of Science **46** (1995), 195–204

The set $S = \{(3,5),(5,7),(11,13),\dots\}$ of twin prime pairs has been studied by Brun (1919) and more recent authors. It has never been proved that S is infinite, although the appropriate Hardy-Littlewood conjecture and numerical evidence strongly suggest that it is. Brun showed that the sum B of reciprocals of twin primes converges (unlike the sum of reciprocals of all primes). However, the sum defining B converges very slowly and irregularly.

Nicely's paper gives counts $\pi_2(x)$ of the number of twin prime pairs $(q, q+2)$ such that $q \le x$, and the corresponding sum of reciprocals $B(x)$, for various $x \le 10^{14}$. The most extensive previously published computation, by the reviewer (1976), went only to $x = 8 \times 10^{10}$.

Many of Nicely's values of $\pi_2(x)$, including those for $x = 10^{13}(10^{13})10^{14}$, have been confirmed in an independent computation performed by J. Kutrib and J. Richstein (personal communication from J. Richstein, September 21, 1995). Similarly for $B(x)$ (to at least 16 decimal places). We record Nicely's values

$$\pi_2(10^{14}) = 135780321665$$