MATHEMATICS OF COMPUTATION
VOLUME 40, NUMBER 162
APRIL 1983, PAGES 685–707

The Discriminant of a Quadratic Extension of an Algebraic Field

By Theresa P. Vaughan

Abstract. Let F be an algebraic field, and K an extension of F of degree 2. We describe a method for computing the relative discriminant D for K over F. We work out the details for the case when F is quadratic and give tables which yield D very easily. We also apply the method to one type of cubic field F, and give tables for it.

1. Introduction. Let F be an algebraic number field, and K an extension of F, of degree 2 over F. We seek a "practical" method of computing the relative discriminant D of K over F.

Suppose $K = F(\sqrt{\gamma})$, where γ is an integer in F; we write (γ) for the principal ideal generated by γ in the ring R of integers of F. Put $D = 2^k D_1$ where D_1 is odd. If p is an odd rational prime and P is a prime ideal divisor of (p) in R, we must discover whether P divides (γ) to an even or odd power. Then (Theorem 3.4) D_1 is the product of all norms of such ideals P, which divide (γ) to an odd power. Thus, the difficulty of finding D_1 is about the same as that of factoring (γ).

The determination of the integer k is rather more complicated. In Section 4, we show the following:

(a) There is a γ_1 in R so that γ/γ_1 is a square in F and (γ_1) is not contained in the square of any prime factor of (2) in R;

(b) There is a β in R so that $\beta^2\gamma_1$ is congruent to a square modulo 4, and β satisfies certain minimality conditions:

(c) 2^k divides the norm of $\beta^2\gamma_1$ exactly (Theorem 4.6).

In actual computation, most of the action takes place in $R/(4)$. If $[F: Q] = n$, then $|R/(4)| = 4^n$, and clearly it is desirable to have as many restrictions as possible on the nature of a suitable β. We address this problem in Section 5. The behavior of the squares in $R/(4)$ is of considerable interest, and we investigate this monoid in Section 6.

In Section 7, we discuss the case of a quadratic field $F = Q(\sqrt{n})$. The only case which is not almost trivial is that of $n \equiv 1 \pmod 8$. In Appendix 1, we give tables for some of the arithmetic of $R/(4)$ in case $n \equiv 1 \pmod 8$; Table V of Appendix 1 summarizes the results for all n. With the aid of these tables, one can easily find the relative discriminant; the only computational difficulty lies in finding and factoring the norm of γ. For specific examples, we work out relative discriminants for a list of fields given by D. Shanks in [2].

Received July 21, 1982.
1980 *Mathematics Subject Classification.* Primary 12A05, 12A50.

0025-5718/82/0000-0993/$06.25

In Section 8, we give a partial discussion of the case when F is a cubic field. The monoid of squares in $R/(4)$ is completely determined (up to isomorphism) by the factorization of (2) in R; we give tables for these monoids in Appendix 2. We work out the details for the field $F = Q(\alpha)$ where α is a root of $x^3 + 2x^2 + 1$. (Here we have $(2) = PQ$; this type is of moderate difficulty; the worst case is when (2) splits.) Note that if $g(x) \in Z[x]$ and $g(x)$ is irreducible and congruent to $x^3 + 2x^2 + 1 \pmod 4$, then all the work done for $Q(\alpha)$ carries over, mutatis mutandis, to $Q(\beta)$ where β is a root of $g(x)$.

In a later paper we hope to complete the work begun in Section 8, and give a complete discussion of all the types of cubic fields.

2. Preliminaries. Let $F = Q(\alpha)$ be an extension of Q of degree n, where α is a root of an irreducible monic polynomial with integer coefficients,

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + x^n.$$

The *conjugates* of α are the roots of $f(x)$ in C; we denote these by $\alpha^{(i)}$ $(i = 1, 2, \ldots, n)$. The *trace* and *norm* of α are defined by

$$\mathrm{Tr}(\alpha) = \sum_{i=1}^{n} \alpha^{(i)}; \qquad N(\alpha) = \prod_{i=1}^{n} \alpha^{(i)},$$

and one has $\mathrm{Tr}(\alpha) = -a_{n-1}$ and $N(\alpha) = (-1)^n a_0$.

All of the following material may be found, in one form or another, in [1].

Let R be the ring of algebraic integers in F. Let $\mathfrak{A} = \{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ be a basis for F over Q, with $\alpha_i \in R$ $(i = 1, 2, \ldots, n)$, and let A be the matrix whose (i, j) entry is $\alpha_j^{(i)}$.

Then the *discriminant* of $\mathfrak{A}$ is $\mathrm{disc}\,\mathfrak{A} = |A|^2$. If $\mathfrak{A}$ is an integral basis for R, then $\mathrm{disc}\,\mathfrak{A} = \mathrm{disc}\,R$, and otherwise, $\mathrm{disc}\,\mathfrak{A} = k^2\,\mathrm{disc}\,R$ where $k \in Z$, $k > 1$.

Now let K be a quadratic extension of F, and let S be the ring of integers in K. Then for some γ in F, with γ not a square in F, we have $K = F(\sqrt{\gamma})$. Evidently, one may assume without loss of generality, that $\gamma \in R$.

Suppose that $\varepsilon = (\beta + \delta\sqrt{\gamma})/j \in S$, where $\beta, \delta \in R$ and $j \in Z$. Define the set $\mathfrak{B}$ by

$$\mathfrak{B} = \{\alpha_1, \alpha_2, \ldots, \alpha_n, \varepsilon\alpha_1, \varepsilon\alpha_2, \ldots, \varepsilon\alpha_n\}.$$

2.1. LEMMA. *With all notation as above, if* $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$ *is an integral basis for* R, *then*

$$\mathrm{disc}\,\mathfrak{B} = (\mathrm{disc}\,R)^2 \cdot \left(\frac{2}{j}\right)^{2n} \cdot N(\delta^2\gamma).$$

Proof. See [1, p. 43]. □

Finally, we use the following notation. If $p, n \in Z$ and p is prime, then $p^t \| n$ means that $p^t \mid n$ and $p^{t+1} \nmid n$. If $\beta \in R$, then (β) is the principal ideal generated by β. If P is a prime ideal in R, then $P^t \| (\beta)$ means that $\beta \in P^t$ and $\beta \notin P^{t+1}$.

3. A Reduction Process. Define the equivalence relation $\sim$ on F^* by $\gamma_1 \sim \gamma_2$ if and only if $\gamma_1 \cdot \gamma_2^{-1}$ is a square in F. Let $[\gamma]$ denote the equivalence class of γ.

3.1. *Definition.* Let $\gamma \in F^*$ and suppose p is a rational prime. Then there exists some $\gamma_1 \in [\gamma]$ satisfying:

(a) $\gamma_1 \in R$,

(b) $p^t \| N(\gamma_1)$ $(t \geqslant 0, t \in Z)$,

(c) If $\gamma_2 \in [\gamma] \cap R$ and if $p^s \| N(\gamma_2)$, then $t \leqslant s$.

Such a γ_1 is said to be *reduced relative to p*.

3.2. LEMMA. *Let $\gamma \in R$, and let p be a rational prime, where $\{P_i: i = 1, 2, \ldots, k\}$ is the set of the prime ideal divisors of (p) in R. Then for any $i = 1, 2, \ldots, k$, $\gamma \in P_i^2$ if and only if there exists some $k \in Z$ with $(k, p) = 1$, and some $\delta \in R$ such that $P_i \| (\delta)$, and $P_j \nmid (\delta)$ if $i \neq j$, such that*

$$k^2\gamma = \delta^2\gamma_1$$

for some γ_1 in R.

Proof. Fix i, and put $P = P_i$. Choose δ as described above. Then there exists $\varepsilon \in R$ so that $\delta\varepsilon = pk$, where $k \in Z$ and $(k, p) = 1$ (ε is in the conjugate of P). Then, if $\gamma \in P^2$, we have

$$\varepsilon^2\gamma = p^2 \cdot \gamma_1$$

for some γ_1 in R, and hence, multiplying both sides by δ^2, we have $k^2\gamma = \delta^2 \cdot \gamma_1$ as required. The converse is obvious. □

3.3. LEMMA. *Let γ and p be as in Lemma 3.2. Then γ is reduced relative to p if and only if $\gamma \notin P_i^2$ $(i = 1, 2, \ldots, k)$.*

Proof. Suppose first that $\gamma \in P_i^2$ for some i. Then by Lemma 3.2 we have $k^2\gamma = \delta^2\gamma_1$ where $(k, p) = 1$, $P_i \| (\delta)$, and $P_j \nmid (\delta)$ if $i \neq j$. Then $\gamma \sim \gamma_1$, and if $p^u \| N(\gamma)$ and $p^v \| N(\gamma_1)$, clearly $v < u$. Then γ is not reduced relative to p.

On the other hand, suppose $\gamma \notin P_i^2$ for any i, and $\gamma \sim \gamma_1$ where γ_1 is reduced relative to p. By the above, we know $\gamma_1 \notin P_i^2$ for any i, and we also have $\alpha^2\gamma = \beta^2\gamma_1$ for some $\alpha, \beta \in R$. Then $P_i^{2r+1} \| (\alpha^2\gamma)$ is possible if and only if $P_i \| (\gamma)$; since $\alpha^2\gamma = \beta^2\gamma_1$, we have $P_i \| (\gamma)$ if and only if $P_i \| (\gamma_1)$. Then $N(\gamma)$ and $N(\gamma_1)$ are divisible by exactly the same power of p, and so by definition, since γ_1 is reduced relative to p, so is γ. □

If p is an odd prime, the situation is easily described.

3.4. THEOREM. *Let p be an odd prime and $\gamma \in F$, where γ is not a square in F, and γ is reduced relative to p. Suppose that $p^t \| \operatorname{disc} R$ and $p^s \| N(\gamma)$. Then $p^{2t+s} \| \operatorname{disc} S$.*

Proof. Since $p > 2$, we need only show that if $\alpha, \beta \in R$, then $(\alpha + \beta\sqrt{\gamma})/p \notin S$ unless $(p) | (\alpha)$ and $(p) | (\beta)$ (Lemma 1.1). Thus suppose that $(\alpha + \beta\sqrt{\gamma}) = p\varepsilon$ for some $\varepsilon \in S$. Then also $(\alpha - \beta\sqrt{\gamma}) = p\varepsilon_1$ for some $\varepsilon_1 \in S$. Since $2\alpha = p(\varepsilon + \varepsilon_1)$ and p is odd, then $(p) | (\alpha)$. Then $\alpha^2 - \beta^2\gamma \in (p^2)$ implies that $\beta^2\gamma \in (p^2)$. But since γ is reduced relative to p, (γ) is not divisible by the square of any prime factor of (p). Then $(p) | (\beta)$ also. The result follows from Lemma 1.1. □

4. The Case $p = 2$. Not surprisingly, this case requires special treatment, beginning with another definition.

4.1. *Definition.* Let $\gamma \in R$ be reduced relative to 2, and not square in F. Choose $\beta \in R$ as follows:

(i) For some $\alpha \in R$, $\alpha^2 - \beta^2\gamma \equiv 0 \pmod 4$.

(ii) $2^t \| N(\beta^2\gamma)$.

(iii) If $\varepsilon, \delta \in R$ and if $\varepsilon^2 - \delta^2\gamma \equiv 0 \pmod 4$ and if $2^s \| N(\delta^2\gamma)$, then $t \leqslant s$.
We say that such a β^2 is a *match* for γ.

This section is devoted to proving that $2^t \| (\operatorname{disc} S)/(\operatorname{disc} R)^2$. We assume throughout the rest of the paper that

$$(2) = P_1^{e_1} P_2^{e_2} \cdots P_r^{e_r}$$

in R, where the P_i are prime ideals.

4.2. LEMMA. (a) *Let $\alpha, \beta \in R$. Then $\alpha^2 \equiv \beta^2 \pmod 4$ if and only if $\alpha \equiv \beta \pmod 2$.*

(b) *Suppose $P_i^{a_i} \| (\alpha)$ and $P_i^{b_i} \| (\beta)$ for $i = 1, 2, \ldots, r$, and let k be a positive integer. Suppose that $0 \leqslant a_i, b_i \leqslant ke_i$ for $i = 1, 2, \ldots, r$. Then $\alpha \equiv \beta \pmod{2^k}$ implies $a_i = b_i$ for $i = 1, \ldots, r$.*

Proof. (a) Let $\alpha^2 - \beta^2 = 4\varepsilon$ for some ε in R. If $P_i^a \| (\alpha - \beta)$ and $P_i^b \| (\alpha + \beta)$, then $a + b \geqslant 2e_i$ and hence (say) $a \geqslant e_i$. Since $\alpha - \beta \equiv \alpha + \beta \pmod 2$, then also $b \geqslant e_i$, and we have $\alpha \equiv \beta \pmod 2$. The converse is obvious.

(b) Put $\delta = \alpha - \beta$, and suppose that, for some i, $a_i < b_i \leqslant ke_i$. Then $\delta \in P_i^{a_i} - P_i^{a_i+1}$, and since $a_i < ke_i$, then $\delta \notin (2^k)$, a contradiction. □

4.3. LEMMA. *Let $\alpha, \beta, \gamma \in R$. Then $(\alpha \pm \beta\sqrt{\gamma})/2 \in S$ if and only if $(\alpha^2 - \beta^2\gamma)/4 \in R$.*

Proof. First suppose that $\alpha^2 - \beta^2\gamma = 4\varepsilon$ in R. Then in S, we have $\beta^2\gamma = (\beta\sqrt{\gamma})^2 = \beta_1^2$, and then $\alpha^2 - \beta_1^2 \equiv 0 \pmod 4$ in S implies $\alpha \equiv \pm\beta_1 \pmod 2$ in S, by Lemma 4.2. That is, $(\alpha \pm \beta\sqrt{\gamma})/2 \in S$.

Conversely, if $(\alpha \pm \beta\sqrt{\gamma})/2 \in S$, then the conjugate $(\alpha \mp \beta\sqrt{\gamma})/2$ is also in S. Then the product $(\alpha^2 - \beta^2\gamma)/4$ is in S. But this product is in F, so it is in R. □

4.4. LEMMA. *Let γ be reduced relative to 2, and suppose for some α, β in R we have $(\alpha + \beta\sqrt{\gamma})/2$ in S. Then $(\alpha + \beta\sqrt{\gamma})/4$ is* **not** *in S unless $\alpha = 2\alpha_1$ and $\beta = 2\beta_1$ for some α_1, β_1 in R.*

Proof. Suppose $(\alpha + \beta\sqrt{\gamma})/4 \in S$. Then also the conjugate $(\alpha - \beta\sqrt{\gamma})/4 \in S$, so $\alpha/2 \in S$. Since $\alpha/2 \in F$, this gives $\alpha = 2\alpha_1$ for some $\alpha_1 \in R$. Suppose next that $\beta/2 \notin R$. That is

$$(\beta) = P_1^{b_1} P_2^{b_2} \cdots P_r^{b_r} X \qquad (0 \leqslant b_i, i = 1, 2, \ldots, r),$$

where X is an ideal of odd norm, and for at least one i, $b_i < e_i$. Since γ is reduced relative to 2, we know that $P_i^{g_i} \| (\gamma)$, where $g_i = 0$ or 1, for $i = 1, 2, \ldots, r$. Then we have $P_i^{2b_i + g_i} \| (\beta^2\gamma)$ where for at least one i, $b_i < e_i$, and $2b_i + g_i < 2e_i$. Hence $(\beta^2\gamma) \not\subset (4)$, that is $\beta^2\gamma/4 \notin R$. But now, we can write $(2\alpha_1 + \beta\sqrt{\gamma})/2 \in S$, which gives $\beta\sqrt{\gamma}/2 \in S$ and $\beta^2\gamma/4 \in R$, a contradiction. Thus we must have $\beta = 2\beta_1$. □

4.5. LEMMA. *Let $s \in R$, and suppose that $P_i^{s_i} \| (s)$ $(i = 1, \ldots, r)$. Choose $\beta_i \in P_i$ so that: $P_i \| (\beta_i)$ and $P_j \nmid (\beta_i)$ if $i \neq j$; for $i = 1, 2, \ldots, r$. Then*

(a) *There exists x in R with odd norm, such that*

$$s \equiv x\beta_1^{s_1}\beta_2^{s_2} \cdots \beta_r^{s_r} \pmod 4.$$

(b) *There exists s' in R such that $s \equiv s' \pmod 2$, and y in R with odd norm, such that*

$$s' = y\beta_1^{u_1}\beta_2^{u_2} \cdots \beta_r^{u_r},$$

where $u_i = \min(s_i, e_i)$ for $i = 1, 2, \ldots, r$.

Proof. (a) For each β_i, we can find $\delta_i \in R$ so that $\beta_i \cdot \delta_i = 2m_i$, where m_i is an odd rational integer. Since $m_i \equiv \pm 1 \pmod 4$, (a) follows from successive applications of the process described in Lemma 3.2. To see (b), use the expression from (a). If $s_i \leqslant e_i$, then $u_i = s_i$: if $s_i > e_i$, $\varepsilon_i = \beta_i^{s_i} + 2$ has $P_i^{e_i} \| (\varepsilon_i)$, $P_j | (\varepsilon_i)$ if $i \neq j$, and by (a) we can write $\varepsilon_i \equiv \beta_i^{e_i} x_i \pmod 4$, where x_i is some integer of odd norm. Substituting ε_i in the expression from (a), for all i for which $e_i < s_i$, we get (b).

At last, we are in a position to prove:

4.6. THEOREM. *Suppose that γ is reduced relative to 2, that γ is not square in F, and that β^2 is a match for γ, with $2^t \| N(\beta^2\gamma)$. Then $2^t \| (\operatorname{disc} S)/(\operatorname{disc} R)^2$.*

Proof. There is some α in R so that $\alpha^2 - \beta^2\gamma \equiv 0 \pmod 4$, so by Lemma 4.3, $(\alpha + \beta\sqrt{\gamma})/2$ is in S. Using the notation of Lemma 1.1 with $j = 2$, we have $\operatorname{disc} \mathfrak{B} = (\operatorname{disc} R)^2 N(\beta^2\gamma)$. The result will follow if we can show that, for all u, s in R, if $X = (u + s(\alpha + \beta\sqrt{\gamma})/2)/2$ is in S, then $u = 2u_1$ and $s = 2s_1$ in R. Thus suppose that $X \in S$. By Lemma 4.5(b) it is clear we may assume that, if for any $i = 1, 2, \ldots, r$ we have $P_i^j \| (\beta)$, then $j \leqslant e_i$, or if $P_i^j \| (s)$ then $j \leqslant e_i$. Since

$$X = \left((2u + s\alpha) + s\beta\sqrt{\gamma}\right)/4 \in S,$$

it follows from Lemma 4.4 that $s\alpha = 2\alpha_1$ and $s\beta = 2\beta_1$ for some α_1, β_1 in R.

Suppose that $P_i^{s_i} \| (s)$ and $P_i^{b_i} \| (\beta)$, with $s_i \leqslant e_i$, $b_i \leqslant e_i$, for $i = 1, 2, \cdots, r$. Then $s\beta = 2\beta_1$ implies that $b_i + s_i \geqslant e_i$ $(i = 1, 2, \ldots, r)$; or

$$s_i = e_i - b_i + w_i \qquad (0 \leqslant w_i \leqslant b_i).$$

So we have $P_i^{w_i} \| (\beta_1)$.

Next, from Lemma 4.3, we get

$$(u + \alpha_1)^2 - \beta_1^2\gamma \equiv 0 \pmod 4;$$

say $2^v \| N(\beta_1^2\gamma)$. If any of the w_i were less than b_i, we would have $v < t$, contradicting the choice of β. Thus every $w_i = b_i$, and then every $s_i = e_i$, so that $s = 2s_1$ for some s_1 in R. Now also we have $2u/4$ in S, that is, $u = 2u_1$, and this completes the proof. □

5. Some Refinements. As it stands, Theorem 4.6 does not look very useful, since the squares in R fall in 2^n congruence classes (mod 4) and 2^n is rather a large number. In this section we give some conditions that α and β must satisfy in order that $\alpha^2 - \beta^2\gamma \equiv 0 \pmod 4$.

5.1. THEOREM. *Suppose that γ is reduced relative to 2, and that $\alpha^2 - \beta^2\gamma \equiv 0 \pmod 4$, and that we have*

$$P_i^{a_i} \| (\alpha), P_i^{b_i} \| (\beta), P_i^{g_i} \| (\gamma) \qquad (i = 1, 2, \ldots, r).$$

(a) *We may assume that $0 \leqslant a_i, b_i \leqslant e_i$.*

(b) *For $i = 1, 2, \ldots, r$, $a_i = b_i$, and if $g_i = 1$, then $a_i = b_i = e_i$.*

Proof. Part (a) follows from Lemma 4.5(b), and (b) from (a) and Lemma 4.2(b). □

5.2. LEMMA. *Suppose that α, β are in R and that $P_i^{a_i} \| (\alpha)$ and $P_i^{a_i} \| (\beta)$ for $i = 1, 2, \ldots, r$. Then there exists some $x \in R$ with odd norm, such that $\alpha^2 \equiv x^2 \cdot \beta^2 \pmod 4$.*

Proof. Lemma 4.2(a) and Lemma 4.5(b). □

5.3. COROLLARY. *Let α, β, γ be as usual. Then $\alpha^2 - \beta^2\gamma \equiv 0 \pmod 4$ if and only if there exist x, y in R, both having odd norm, such that*

(i) $\beta^2(x^2 - \gamma) \equiv 0 \pmod 4$,

(ii) $\alpha^2(1 - y^2\gamma) \equiv 0 \pmod 4$. □

5.4. THEOREM. *Let γ be reduced relative to 2, and suppose that β^2 is a match for γ, with $\alpha^2 - \beta^2\gamma \equiv 0 \pmod 4$. Suppose that α_1 and β_1 in R also satisfy $\alpha_1^2 - \beta_1^2\gamma \equiv 0 \pmod 4$. Finally suppose that*

$$P_i^{b_i} \| (\beta) \quad \text{and} \quad P_i^{c_i} \| (\beta_1) \qquad (i = 1, 2, \ldots, r).$$

Then for $i = 1, 2, \ldots, r$, $0 \leq b_i \leq c_i$.

Proof. We use Theorem 4.6. The basis $\mathfrak{B}$ defined there is not necessarily an integral basis for S, but we do have that $(\operatorname{disc} \mathfrak{B})/(\operatorname{disc} S)$ is an odd integer. Then, putting $\varepsilon = (\alpha + \beta\sqrt{\gamma})/2$, every integer in S can be written in the form $(u + v\varepsilon)/m$, where u, v are in R and m is an odd rational integer.

By Lemma 4.3, we have $(\alpha_1 + \beta_1\sqrt{\gamma})/2$ in S, and thus, for some u, v in R and odd m in Z, we can write

$$u + v\varepsilon = m\left(\alpha_1 + \beta_1\sqrt{\gamma}\right)/2,$$

and hence $m\alpha_1 = 2u + v\alpha$ and $m\beta_1 = v\beta$. Since m is odd, we are done. □

5.5. COROLLARY. (i) *Let γ be reduced relative to 2 and suppose that $\alpha^2 - \beta^2\gamma \equiv 0 \pmod 4$ for some α, β in R. Then $\beta \equiv 0 \pmod 2$* **unless** *there exists x in R with odd norm so that*

$$x^2 - \gamma \equiv 0 \left(\operatorname{mod} P_1^{2a_1} P_2^{2a_2} \cdots P_r^{2a_r}\right)$$

for some integers a_i satisfying $0 \leq a_i \leq e_i$ $(i = 1, \ldots, r)$.

(ii) *If the condition of* (i) *is satisfied, and if β_1^2 is a match for γ, with $P_i^{b_i} \| (\beta_1)$ $(i = 1, 2, \ldots, r)$, then $0 \leq b_i \leq e_i - a_i$ $(i = 1, 2, \ldots, r)$.* □

Remarks. We shall see later that the number N of squares of odd norm, incongruent modulo 4, varies inversely with the number of prime factors of (2) in R. The amount of work we have to do to find a match for some γ depends on N (Corollary 5.3) *and* on the number of factors of (2) (Corollary 5.5). The most manageable cases are those with N small and r close to n, or with (γ) having many of the prime factors of (2) as divisors (Theorem 5.1).

6. The Square-Classes (mod 4) **in** R. Our purpose here is to find out more about the nature of the squares (mod 4) in R, with particular attention to those of odd norm. A square-class $\mathcal{C}$ is defined by

$$\mathcal{C} = \mathcal{C}(x^2) = \{\alpha \in R: \alpha \equiv x^2 \pmod 4\}.$$

Let M be the set of all square-classes in R. The obvious multiplication, $\mathcal{C}(x^2)\mathcal{C}(y^2) = \mathcal{C}(x^2y^2)$, makes M a monoid, with identity $\mathcal{C}(1)$; by Lemma 4.2 we have $|M| = 2^n$. Many of the results of previous sections can be restated as properties of M and we list these without proof.

Let U be the set of invertible elements in M. That is,

$$U = \{\mathcal{C}(x^2)\colon N(x) \text{ is odd}\}.$$

Evidently, U is a group.

Choose $\beta_i \in P_i$ so that $P_i \| (\beta_i)$ and $P_j \nmid (\beta_i)$ if $i \neq j$. Then each product of the form

$$\delta = \prod_{i=1}^{r} \beta_i^{t_i} \qquad (0 \leqslant t_i \leqslant e_i)$$

gives rise to a square class $\mathcal{C}(\delta^2)$, and these classes are distinct. Let D be the set of all these classes. Then

6.1. THEOREM. *Let $\mathcal{C}$ be any square-class. Then there exist x, δ in R so that $\mathcal{C}(x^2) \in U$ and $\mathcal{C}(\delta^2) \in D$ and $\mathcal{C} = \mathcal{C}(x^2)\mathcal{C}(\delta^2)$. (We shall say that $\mathcal{C}$ is* **associated** *with the r-tuple $(t_1, t_2, \ldots, t_r)$.)*

We define two sets for every square-class in M:

$$U(\mathcal{C}) = \{\mathcal{C}(x^2)\colon N(x) \text{ is odd and } \mathcal{C}(x^2)\mathcal{C} = \mathcal{C}\},$$

$$F(\mathcal{C}) = \{\mathcal{C}(x^2)\mathcal{C}\colon N(x) \text{ is odd}\}.$$

6.2. LEMMA. *Suppose that $\mathcal{C}_1$ and $\mathcal{C}_2$ in M are associated to the same r-tuple $(t_1, \ldots, t_r)$. Then $\mathcal{C}_1 \in F(\mathcal{C}_2)$.*

6.3. THEOREM. *Let γ be reduced relative to 2, and suppose β^2 is a match for γ. Then there exists α in R such that $\alpha^2 - \beta^2\gamma \equiv 0 \pmod 4$, and $\mathcal{C}(\alpha^2) \in F(\mathcal{C}(\beta^2))$.*

6.4. THEOREM. (a) *For every $\mathcal{C}$ in M, $U(\mathcal{C})$ is a subgroup of U.* (b) *If $\mathcal{C}_1 \in F(\mathcal{C})$, then $U(\mathcal{C}_1) = U(\mathcal{C})$.* (c) *If $\mathcal{C}_1$ is associated to $(t_1, t_2, \ldots, t_r)$ and $\mathcal{C}_2$ to $(s_1, \ldots, s_r)$, and if $t_1s_1 + t_2s_2 + \cdots + t_rs_r = 0$, then $U(\mathcal{C}_1) \cap U(\mathcal{C}_2) = \{\mathcal{C}(1)\}$.*

Proof. Parts (a) and (b) follow directly. To see (c), choose $\alpha_1^2 \in \mathcal{C}_1$ and $\alpha_2^2 \in \mathcal{C}_2$, and suppose $\mathcal{C}(x^2) \in U(\mathcal{C}_1) \cap U(\mathcal{C}_2)$. Then $x^2\alpha_1^2 \in \mathcal{C}_1$ and $x^2\alpha_2^2 \in \mathcal{C}_2$, so we have

$$x^2\alpha_1^2 \equiv \alpha_1^2 \pmod 4, \quad x^2\alpha_2^2 \equiv \alpha_2^2 \pmod 4,$$

$$\alpha_1^2(1 - x^2) \equiv 0 \pmod 4, \quad \alpha_2^2(1 - x^2) \equiv 0 \pmod 4,$$

$$(1 - x^2) \equiv 0 \left(\mathrm{mod}\left(\prod_{i=1}^{r} P_i^{e_i - t_i}\right)^2\right) \quad \text{and} \quad (1 - x^2) \equiv 0 \left(\mathrm{mod}\left(\prod_{i=1}^{r} P_i^{e_i - s_i}\right)^2\right).$$

Since $\sum t_i s_i = 0$, it follows that $(1 - x^2) \equiv 0 \pmod{P_i^{2e_i}}$ for all $i = 1, 2, \ldots, r$. Then $(1 - x^2) \equiv 0 \pmod 4$ and $\mathcal{C}(x^2) = \mathcal{C}(1)$.

6.5. THEOREM. *If $|U| = m$, and $|U(\mathcal{C})| = k$, then $|F(\mathcal{C})| = m/k$. We also have*

$$\sum_{\mathcal{C}} |F(\mathcal{C})| = 2^n$$

where the sum is taken over $\mathcal{C}$ such that the sets $F(\mathcal{C})$ are mutually disjoint.

The cardinality of U is the number of units in the ring $R/(2)$ (Lemma 4.2); in case $R \cong Z/(f(x))$ (more or less), this number was given by Dedekind. We provide here the slight generalization to any R.

6.6. *Definition.* If I is an ideal in R, put $\|I\| = |R/I|$, and let $\phi(I)$ be the number of units in R/I.

6.7. THEOREM. ϕ: $I \to \phi(I)$ *is a multiplicative function from the set of ideals in R to Z; that is, if* I_1 *and* I_2 *are relatively prime, then* $\phi(I_1 I_2) = \phi(I_1)\phi(I_2)$.

Proof. We can write

$$I = P_1^{r_1} \cdots P_k^{r_k},$$

where the P_i are prime ideals in R. Then

$$R/I \cong \bigoplus_{i=1}^{k} R/P_i^{r_i}$$

and u is a unit in R/I if and only if, under the isomorphism above, U corresponds to some $(u_1, u_2, \ldots, u_k)$ where u_i is a unit in $R/P_i^{r_i}$ $(i = 1, 2, \ldots, k)$. □

6.8. THEOREM. *If P is a prime ideal in R, and r is a positive integer, then*

$$\phi(P^r) = \|P\|^r \left(1 - \frac{1}{\|P\|}\right).$$

Proof. The chain $R \supset P \supset P^2 \supset \cdots$ projects naturally to $\bar{R} = R/P^r$, giving the chain $\bar{R} \supset \bar{P} \supset \bar{P}^2 \supset \cdots \supset \bar{P}^{r-1} \supset \bar{P}^r = \{0\}$ (where $\bar{P}$ is the unique maximal ideal of $\bar{R}$). Then we have

$$\bar{R} = |\bar{R}/\bar{P}| \cdot |\bar{P}/\bar{P}^2| \cdot |\bar{P}^2/\bar{P}^3| \cdots = \|P\|^r,$$

$$\bar{P} = |\bar{P}/\bar{P}^2| \cdot |\bar{P}^2/\bar{P}^3| \cdots = \|P\|^{r-1}.$$

Since $\bar{P}$ is the unique maximal ideal of $\bar{R}$, then u is a unit in $\bar{R}$ if and only if $u \in \bar{R} - \bar{P}$. Thus the number of units is $\|P\|^r - \|P\|^{r-1}$, as required. □

6.9. COROLLARY. *Let* $(2) = P_1^{e_1} \cdots P_r^{e_r}$, *where* P_i *is a prime ideal of degree* f_i $(i = 1, \ldots, r)$. *Then*

$$|U| = \phi((2)) = 2^n \prod_{i=1}^{r} (1 - 2^{-f_i}).$$

7. Quadratic Fields. We use the same notation as before, and in addition

$$m = (\operatorname{disc} S)/(\operatorname{disc} R)^2.$$

We have $K = F(\sqrt{\gamma})$, where γ is a nonsquare in R; we wish to compute m. In practice, one is often faced with a γ which is not reduced relative to one or more primes; to find the power of prime p dividing m, we need to know something about reduced forms of γ, relative to p. It is not necessary, in general, to find such a form explicitly, as our examples show. Indeed, for odd primes, all we need is the prime ideal factorization of the principal ideal (γ) (Lemma 3.3; Theorem 3.4). If $p = 2$, however, it is also necessary to work with the arithmetic of $R/(4)$. In this section, we work out the details for the case of a quadratic field $F = Q(\sqrt{Z})$, together with an assortment of specific examples borrowed from a paper of Shanks [2]. The results are summarized in Table V of Appendix 1.

Let $F = Q(\sqrt{Z})$, where Z is a squarefree integer. An integral basis for R is $\{1, \omega\}$, where $\omega = \sqrt{Z}$ if $Z \equiv 2, 3 \pmod 4$ and $\omega = (1 + \sqrt{Z})/2$ if $Z \equiv 1 \pmod 4$. We shall denote $a + b\omega$ by (a, b).

7.1. *Case* 1. Let $Z \equiv 2 \pmod 4$. An integral basis for R is $\{1, \sqrt{Z}\}$, and $(2) = P^2$. If $\gamma = a + b\sqrt{Z}$, we can write $\gamma = 2^k(c + d\sqrt{Z})$ where either c or d is odd; $\gamma_1 = c + d\sqrt{Z}$ is reduced relative to 2, and $\gamma \sim \gamma_1$. We have $|U| = 2$ and the "odd squares" are $(1,0)$ and $(3,2) \pmod 4$. If c is odd and d is even, but $\gamma \not\equiv x^2 \pmod 4$, then $(c, d) - (1,0) \in (2) = P^2$ and a match, β^2, will have $2^2 \| \beta^2$. Then $4 \| m$. If c, d are odd, the only match will have $2^4 \| \beta^2$ and then $2^4 \| m$. If c is even, d odd, again the only match has $2^4 \| \beta^2$; since $2 \| N(c + d\sqrt{Z})$ we have $2^5 \| m$.

The case $Z \equiv 3 \pmod 4$ is similar to the above; in this case the "odd squares" are $(1,0)$ and $(3,0)$.

7.2. *Case* 2. Let $Z \equiv 5 \pmod 8$. Then $\omega = (1 + \sqrt{Z})/2$, and $(2) = P$. We can write

$$\gamma = a + b\omega = 2^k(c + d\omega) = 2^k\gamma_1,$$

and if k is even, $\gamma \sim \gamma_1$, while if k is odd, then $\gamma \sim 2\gamma_1$. If $Z = 8j + 5$, the odd squares $(\mathrm{mod}\, 4)$ are: $(1,0)$, $(2j + 1, 1)$, $(2j + 2, 3)$. Then a match for the reduced form of γ is 1 if it is congruent to one of the odd squares $(\mathrm{mod}\, 4)$ and is 4 otherwise.

7.3. *Case* 3. Let $Z \equiv 1 \pmod 8$, so $\omega = (1 + \sqrt{Z})/2$. Now $(2) = PQ$, and the situation is more complicated accordingly. The tables of Appendix 1 give enough of the arithmetic of $R/(4)$ for our purposes; note that (writing $Z = 8y + 1$) there are different tables for y even and y odd. Tables Ia and Ib give some of the multiplication of $R/(4)$. Table II gives the norm modulo 4, for $\gamma \not\equiv 0 \pmod 2$. If γ is already reduced then these tables allow the determination of the power of 2 dividing m; one need only decide if $1 - \gamma$ is in P^2, Q^2, (4), or none of these (Corollary 5.3). The results are in Table V.

The reduction process is more involved, and for this we need Tables III and IV. Suppose $\gamma = n + m\omega$ has even norm and $\gamma \notin (2)$; say $\gamma \in P$. Choose $\beta \in Q$ so that $N(\beta) = 2b$, $b \equiv 1 \pmod 4$. Write $N(n + m\omega) = 2^j x$, x odd. Then $\beta(n + m\omega) = 2(a + b\omega)$; Table III gives the values of (a, b). Note that we need to know whether x is congruent to 1 or 3 mod 4 to take care of the case when j is even. For Table IV, we have $X = 2(n + m\omega)$ where $N(n + m\omega) = 2x$, x odd. Choose β as for Table III; then $X\beta^2 = 4(a + b\omega)$. In Table III, if $j \geqslant 4$, and if $\beta^2(n + m\omega) = 4(u + v\omega)$, then $(n, m) \equiv (u, v) \pmod 2$, so that in fact this process is reasonably short.

7.4. *Examples.* As an illustration, we find the value of m for some quartic fields discussed by Daniel Shanks in [2]. The situation is this: Let $T = X + Y\sqrt{Z}$ and $t = T + \sqrt{T^2 - 1}$, where Shanks' requirements are that $Z, 4X$, and $4(X^2 - Y^2Z)$ are integers, and $|X - Y\sqrt{Z}| < 1$. Then t is a root of the reciprocal polynomial:

$$f(y) = y^4 - 4Xy^3 + \big(2 + 4(X^2 - Y^2Z)\big)y^2 - 4Xy + 1.$$

Dr. Shanks has shown that

$$\mathrm{disc}(f) = \big((4Y)^2Z\big)^2 f(1)f(-1)$$

(personal communication), but it is not very easy to find the value of m from this; in practice $\mathrm{disc}\, f$ seems to have a lot of extraneous factors. It is easier to tackle $\gamma = T^2 - 1$ directly. Below, we give the values of m for most of the examples listed in [2]. We do two of these in detail, and for the rest we indicate the main steps.

(A) Let $A = (13 + \sqrt{193})/2$. Then $Z = 8 \cdot 24 + 1$, and $y = 24$ is even. We have $A = 6 + \omega$ and $A^2 - 1 = (A - 1)(A + 1) = (5 + \omega)(7 + \omega)$. Mod 4, this is $A^2 - 1 \equiv (1, 1) \cdot (3, 1) = (3, 1)$ (Table Ia). One computes $N(A - 1) = -18$, $N(A + 1) = 8$, so $N(A^2 - 1) = 2^4(-9)$; for our tables, $j = 4$ and $x = -9 \equiv 3 \pmod 4$. Then four multiplications by a suitable β yield the sequence

$$(3, 1) \overset{\beta^2}{\to} (3, 1) \overset{\beta}{\to} (1, 1) \overset{\beta}{\to} (3, 2).$$

We use Table III; observe that it is not necessary to carry out any actual calculations, nor to know anything more about β than that it exists. So $\gamma = A^2 - 1 \sim \gamma_1$ where $\gamma_1 \equiv (3, 2) \pmod 4$. From Table V, $4 \parallel m$; alternatively, from Table Ia we see that $(3, 2) \cdot (0, 1) = (0, 1) = (2, 1)^2$ and a match for γ_1 is $\beta^2 \equiv (2, 1)^2 \pmod 4$, with $2 \parallel N(\beta)$. $N(\gamma_1)$ is odd, so $4 \parallel N(\beta^2\gamma_1)$ and $4 \parallel m$. Finally, 3 is not ramified in F, and $A^2 - 1 \not\equiv 0 \pmod 3$ so we have $\gamma \sim \gamma_2$ where $3 \nmid N(\gamma_2)$; hence $3 \nmid m$. The factor -1 is not square, so $m = -4$.

(B) Let $B = (25 + \sqrt{697})/4 = (12 + \omega)/2$. We have $697 = 8 \cdot 87 + 1$; y is odd. Since $B^2 - 1 \sim 4B^2 - 4$, we use $2B - 2 = 10 + \omega \equiv (2, 1)$ and $2B + 2 = 14 + \omega \equiv (2, 1)$; $N(2B - 2) = -2^6$ and $N(2B + 2) = 36$; $N(4B^2 - 4) = 2^8(-9)$; $j = 8$, $x = -9 \equiv 3 \pmod 4$. We have $(2, 1) \cdot (2, 1) = (2, 1)$, and the sequence is

$$(2, 1) \underset{\beta^6}{\to} (2, 1) \underset{\beta}{\to} (0, 3) \underset{\beta}{\to} (3, 2)$$

and as before, $4 \parallel m$, $3 \nmid m$, and $m = -4$.

The remaining examples from [2] are given below in tabular form.

8. Cubic Fields. We use the notation of the previous sections, where now F is a cubic extension of Q. Then $|R/(4)| = 64$, $|R/(2)| = 8$, and there are eight equivalence classes of squares (mod 4). The structure of the monoid M is determined, up to isomorphism, by the factorization of (2) in F. (Since F is a cubic field, this is an easy consequence of the results of Section 6; it is also easy, if tedious, to show this directly.) When $(2) = P$, a prime in F, then $M - \{0\}$ is a cyclic group of order 7; for all other cases, we give the tables for M in Appendix 2.

We seek the power of 2 dividing $m = (\operatorname{disc} S)/(\operatorname{disc} R)^2$. The situation is foreshadowed, to some degree, by the quadratic case: if γ is already reduced relative to 2, it is comparatively simple to discover this power of 2, while if γ is not reduced, some sort of reduction process is needed. If (2) has only one prime factor, reduction is a simple matter; if (2) has two prime factors there are some manageable difficulties. If (2) has three distinct factors, we have found (so far) only a partial solution to the reduction problem. We shall work out one comparatively simple case, with $(2) = PQ$. The necessary tables are given in Appendix 3. The methods used for the quadratic case are not sufficient here, doubtless reflecting the fact that the two factors of (2) are not of the same degree; nevertheless there is considerable similarity.

T	$J = 226 + 25\sqrt{82}$	$K = (225 + 25\sqrt{82})/2$	$L = (459 + 325\sqrt{2})/2$	$M = (195 + 137\sqrt{2})/2$
$2T - 2 \quad (T - 1)$ norm type	$225 + 25\sqrt{82}$ $= 25(9 + \sqrt{82}) \sim 9 + \sqrt{82} - 1$ $(1, 1)$	$223 + 25\sqrt{82}$ -9×13^2 $(3, 1)$	$457 + 325\sqrt{2}$ -7^4 $(1, 1)$	$193 + 137\sqrt{2}$ -17^2 $(1, 1)$
$2T + 2 \quad (T + 1)$ norm type	$227 + 25\sqrt{82}$ 9×31 $(3, 1)$	$227 + 25\sqrt{82}$ 9×31 $(3, 1)$	$461 + 325\sqrt{2}$ 31×41 $(1, 1)$	$197 + 137\sqrt{2}$ 31×41 $(1, 1)$
y	$--$	$--$	$--$	$--$
x	$--$	$--$	$--$	$--$
sequence	$(3, 1) \times (1, 1) = (1, 0); 2 \nmid m$	$(3, 1)^2 = (3, 2); 2 \nmid m$	$(1, 1)^2 = (3, 2); 2 \nmid m$	$(1, 1)^2 = (3, 2); 2 \nmid m$
m	-31	-31	-31×41	-31×41

T	$P = (621 + 49\sqrt{161})/2$	$Q = (321 + 25\sqrt{161})/4$	$R = (393 + 31\sqrt{161})/4$	$S = (2529 + 199\sqrt{161})/4$
$2T - 2 \quad (T - 1)$ norm type	$285 + 49\omega$ $2 \times (-17 \times 25)$ $(1, 1)$	$146 + 25\omega$ $2 \times (-17)$ $(2, 1)$	$179 + 31\omega$ $2 \times (-25 \times 17)$ $(3, 3)$	$1163 + 199\omega$ $2 \times (-17)$ $(3, 3)$
$2T + 2 \quad (T + 1)$ norm type	$287 + 49\omega$ 8×49 $(3, 1)$	$25(6 + \omega) \sim (6 + \omega)$ 2 $(2, 1)$	$183 + 31\omega$ 2×19^2 $(3, 3)$	$1167 + 199\omega$ 2×71^2 $(3, 3)$
y	20	20	20	20
x	$-17 \times 5^2 \times 7^2 \equiv 3(4)$	$-17 \equiv 3(4)$	$\equiv 3(4)$	$\equiv 3(4)$
sequence	$(3, 1) \to (3, 1) \to (1, 1) \to (3, 2)$	$(0, 1) \to (2, 3) \to (3, 2)$	$(1, 3) \to (3, 3) \to (1, 2)$	$(1, 3) \to (3, 3) \to (1, 2)$
m	-4×17	-4×17	-4×17	-4×17

T	$J = (15 + \sqrt{137})/4$	$K = (9 + \sqrt{137})/4$	$L = (263 + 16\sqrt{274})/2$	$M = (233 + 14\sqrt{274})/2$
$2T-2 \quad (T-1)$ norm type	$5 + \omega$ -4 $(1,1)$	$2 + \omega$ -4×7 $(2,1)$	$261 + 16\sqrt{274}$ -7×17^2 $(1,0)$	$231 + 14\sqrt{274} = 7(33 + 2\sqrt{274})$ -7^3 $(3,2)$
$2T+2 \quad (T+1)$ norm type	$9 + \omega$ 7×8 $(1,1)$	$6 + \omega$ 8 $(2,1)$	$265 + 16\sqrt{274}$ 81 $(1,0)$	$235 + 14\sqrt{274}$ 9×13^2 $(3,2)$
y	17	17	$--$	$--$
x	$\equiv 1(4)$	$\equiv 1(4)$	$--$	$--$
sequence	$(3,3) \to (3,3) \to (1,1) \to (3,1)$	$(2,1) \to (2,1) \to (2,1) \to (0,3)$	$(1,0)^2 = (1,0);\ 2 \nmid m$	$(3,2)^2 = (1,0),\ 2 \nmid m$
m	-7×8	-7×8	-7	-7

T	$J = (213 + 23\sqrt{89})/4$	$K = (69 + 7\sqrt{89})/4$	$L = (93 + 23\sqrt{17})/2$	$M = (129 + 31\sqrt{17})/4$
$2T-2 \quad (T-1)$ norm type	$93 + 23\omega$ $2 \cdot (-25 \times 17)$ $(1,3)$	$29 + 7\omega$ $2 \cdot (-17)$ $(1,3)$	$34 + 23\omega$ $2 \cdot (-89)$ $(2,3)$	$47 + 31\omega$ $2 \cdot (-89)$ $(3,3)$
$2T+2 \quad (T+1)$ norm type	$97 + 23\omega$ 2 $(1,3)$	$33 + 7\omega$ 2×11^2 $(1,3)$	$36 + 23\omega$ 8 $(0,3)$	$51 + 31\omega$ 2×13^2 $(3,3)$
y	11	11	2	2
x	$\equiv 3(4)$	$\equiv 3(4)$	$\equiv 3(4)$	$\equiv 3(4)$
sequence	$(3,3) \to (1,3) \to (1,2)$	$(3,3) \to (1,3) \to (1,2)$	$(0,3) \to (0,3) \to (2,1) \to (1,2)$	$(1,3) \to (3,3) \to (1,2)$
m	-4×17	-4×17	-4×89	-4×89

T	$T_1 = (242 + 23\sqrt{109})/2$	$T_2 = (176 + 17\sqrt{109})/2$	$T_3 = (199861 + 2451\sqrt{6649})/4$	$T_4 = (147837 + 1813\sqrt{6649})/4$
$2T-2 \quad (T-1)$ norm type	$217 + 46\omega$ -61 $(1,2)$	$157 + 34\omega$ -25×49 $(1,2)$	$98703 + 2451\omega$ $-2^4 \times 25 \times 9^2 \times 3$ $(3,3)$	$73010 + 1813\omega$ $-2^4 \times 3 \times 7^4$ $(2,1)$
$2T+2 \quad (T+1)$ norm type	$221 + 46\omega$ $25^2 \times 3$ $(1,2)$	$161 + 34\omega$ 3×61 $(1,2)$	$98707 + 2451\omega$ $4 \times (419)^2$ $(3,3)$	$73014 + 1813\omega$ $4 \times 25 \times 9 \times 23^2$ $(2,1)$
y	$109 \equiv 5(8)$, irrelevant	$--$	831	831
x	$--$	$--$	$\equiv 1(4)$	$\equiv 1(4)$
sequence	$(1,2)^2 = (1,0);\ 2\nmid m$	$(1,2)^2 = (1,0);\ 2\nmid m$	$(3,3) \to (3,3) \to (1,3) \to (1,0)$	$(2,1) \to (2,1) \to (0,3) \to (1,0)$
m	-3×61	-3×61	$m = -3$	$m = -3$

T	$J = (135 + 13\sqrt{113})/4$	$K = (57 + 5\sqrt{113})/4$	$L = (177 + 125\sqrt{2})/2$	$M = (105 + 73\sqrt{2})/2$
$2T-2 \quad (T-1)$ norm type	$59 + 13\omega$ $4 \cdot (-11^2)$ $(3,1)$	$24 + 5\omega$ -4 $(0,1)$	$175 + 125\sqrt{2} \sim 7 + 5\sqrt{2}$ -1 $(3,1)$	$103 + 73\sqrt{2}$ -7^2 $(3,1)$
$2T+2 \quad (T+1)$ norm type	$63 + 13\omega$ 7×8 $(3,1)$	$28 + 5\omega$ $2^5 \times 7$ $(0,1)$	$179 + 125\sqrt{2}$ 7×113 $(3,1)$	$107 + 73\sqrt{2}$ 7×113 $(3,1)$
y	14	14	$--$	$--$
x	$\equiv 1(4)$	$\equiv 1(4)$	$--$	$--$
sequence	$(1,3) \to (1,3) \to (3,1) \to (1,1)$	$(0,1) \to (0,1) \to (0,1) \to (2,3)$	$(3,1)^2 = (3,2);\ 2\nmid m$	$(3,1)^2 = (3,2);\ 2\nmid m$
m	$m = -7 \times 8$	$m = -7 \times 8$	-7×113	-7×113

Let $f(x) = x^3 + 2x^2 + 1$. Then $\operatorname{disc} f = -59$, and (where α is a root of $f(x)$), $\{1, \alpha, \alpha^2\}$ is an integral basis for R. We denote $a + b\alpha + c\alpha^2$ by (a, b, c). The multiplication in R (or in F) is given by $(a, b, c)\cdot(r, s, t) = (x, y, z)$ where:

$$x = ar - cs + (-b + 2c)t,$$
$$y = br + as - ct,$$
$$z = cr + (b - 2c)s + (a - 2b + 4c)t.$$

Let C be the companion matrix for $f(x)$,

$$C = \begin{bmatrix} 0 & 0 & -1 \\ 1 & 0 & 0 \\ 0 & 1 & -2 \end{bmatrix}.$$

The correspondence $g(\alpha) \leftrightarrow g(C)$ is an isomorphism of F with $Q[C]$. We have

$$\beta = (a, b, c) \leftrightarrow B = \begin{bmatrix} a & -c & -b + 2c \\ b & a & -c \\ c & b - 2c & a - 2b + 4c \end{bmatrix}.$$

We shall have some use for the adjoint of B; say $\operatorname{adj} B \leftrightarrow (u, v, w)$, where

$$u = a^2 - 2ab + bc + 4ac + 2c^2,$$
$$v = -c^2 - ab + 2b^2 - 4bc,$$
$$w = b^2 - 2bc - ac.$$

Recall that $|B| = N(\beta)$; $\operatorname{Tr}(B) = \operatorname{Tr}(\beta)$; $|\operatorname{adj} B| = |B|^2$, $B(\operatorname{adj} B) = N(\beta)I$. We investigate only the power of 2 dividing m. Since $f(x) \equiv x^3 + 1 \pmod 2$, then in R, $(2) = PQ$, where we choose $P = (\alpha + 1, 2) = (\alpha + 1)$ and $Q = (\alpha^2 + \alpha + 1, 2) = (\alpha^2 + \alpha + 1)$.

The congruence classes modulo 2, are grouped as follows:

(2)	(000)
P	(110), (101), (011)
Q	(111)
(1)	(100), (010), (001)

If (a, b, c) is given modulo 2, then $(a, b, c)^2 = (x, y, z)$ is determined modulo 4. The square table is:

(a, b, c)	000	100	010	001	110	101	011	111
(x, y, z)	000	100	001	230	121	332	031	113

In the first column of Table I of Appendix 3, we give a list of all $(a, b, c) \not\equiv 0 \pmod 2$, with the left-most entry 1. (All entries are given modulo 4.) The second column gives $(a, b, c)\cdot(001)$ and the third gives $(a, b, c)\cdot(230)$. Thus the elements in any row (in the first three columns) are equivalent mod $\sim$ via multiplicaton by unit squares. Every (a, b, c) is either congruent (mod 4) to one of these, or to a multiple thereof by 0, 2, or 3. Thus we restrict our attention to the twelve entries of the first column.

We need to know which of these are reduced relative to two. If $\beta_1 \equiv \beta_2 \pmod 4$ then $N(\beta_1) \equiv N(\beta_2) \pmod 4$, so the entries of the fourth column tell that all the units are reduced, and also (110) and (132). One checks that (111), (131), (133) are all reduced, and (113) is not.

Next, which γ satisfy: $\gamma \not\equiv 0$ (2), $\beta^2\gamma$ is a square (mod 4), where γ and β are both reduced? We first choose γ by: $\beta \in P$, $1 - \gamma \in Q^2$, and then $\beta \in Q$, $1 - \gamma \in P^2$. We require γ reduced, and not a square (mod 4), so this gives:

(i) $\beta \in P$, $\gamma \in \{(213), (322)\}$,

(ii) $\beta \in Q$, $\gamma = (u, v, w)$ with $u + v + w \equiv 1 \pmod 4$ or $\gamma \in \{(122), (010), (320), (131)\}$.

For every possible γ listed above, we also include every $\gamma' \sim \gamma$ from Table I; for example, with (213) we also have (110) and (303). This set of γ is a complete set satisfying the stated requirements (Corollary 5.3).

From Theorem 5.1, if γ is reduced and $\gamma \equiv 0 \pmod 2$, then a match for γ is $\beta^2 = 2^2$. The only way such a γ can be reduced is if it has the form $2(x, y, z)$ where $N(x, y, z)$ is odd. We have considered all possibilities and the results are listed in Table V.

There remains the problem of finding a reduced form $\gamma' \pmod 4$ for some given γ which is not reduced relative to 2. We shall assume first that $\gamma \not\equiv 0 \pmod 2$. In Table II, we give the result (x, y, z) of multiplying $\gamma \in P$ by (111) and dividing through by two. Each γ gives rise to two possible (x, y, z); where γ is already reduced, one of them has norm congruent to 1 (mod 4) and the other to 3 (mod 4). Where γ is not reduced, one of the (x, y, z) is reduced, and the other is not. Now if $N(\gamma) = 2^j x$, and if $\gamma \sim \gamma'$ where γ' is reduced, then $N(\gamma') \equiv 2 \pmod 4$ if j is odd, and $N(\gamma') \equiv x \pmod 4$ if j is even. Thus we can "chase the table" to a unique result, for $\gamma \in P$, $\gamma \not\equiv 0 \pmod 2$. (We give an example later.)

Unfortunately, for $\gamma \in Q$, the "table approach" does not work unless $N(\gamma) = 4^j x$, x odd, j odd. Of course, we can construct a table, using the multiplier (110) (Table III) but the result is four possibilities for (x, y, z); in case j is even, we have found no simple way to distinguish these in general. We get around the problem by using the adjoint (described earlier). This works equally well whether j is even or odd; here we assume j even. Let $\gamma = (u, v, w)$ so that

$$\gamma \leftrightarrow G = \begin{bmatrix} u & -w & -v + 2w \\ v & u & -w \\ w & v - 2w & u - 2v + 4w \end{bmatrix}.$$

We have $N(\gamma) = 4^j x$ and $\gamma \in Q$. It is shown in [3] that the Smith form S of G has the form

$$S = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 2^j y & 0 \\ 0 & 0 & 2^j z \end{bmatrix},$$

where $y \mid z$ and $yz = x$ (indeed, every $\gamma \in Q$, $\gamma \not\equiv 0 \pmod 2$, must have such a Smith form and conversely). The Smith form S_1 of adj G is then

$$S_1 = 2^j \begin{bmatrix} y & 0 & 0 \\ 0 & z & 0 \\ 0 & 0 & 2^j x \end{bmatrix}.$$

That is, adj $G = 2^j B$, where B is an integral and $B \not\equiv 0 \pmod 2$. We have $B \leftrightarrow (a, b, c)$ and $(a, b, c) \in P$, $(a, b, c) \not\equiv (000) \pmod 2$. We have

$$(uvw) \cdot 2^j(abc) = 4^j x,$$
$$(u, v, w) \cdot (xa, xb, xc) = 2^j x^2.$$

Since j is even, we have $(u, v, w) \sim (xa, xb, xc)$; since x is odd, this is well-determined modulo 4. Finally, since $(xa, xb, xc) \in P$, we can use Table II.

Now suppose $\gamma = 2\gamma_1$, where $\gamma_1 \not\equiv 0 \pmod 2$, and $N(\gamma_1) = 2^t x$ (x odd). If $\gamma_1 \in P$ and t is even, or if $\gamma_1 \in Q$ and $t \equiv 0 \pmod 4$, then we have $\gamma \sim 2\gamma'$ where $N(\gamma')$ is odd, and $2^6 \| m$ from Table V. We now suppose that either $\gamma_1 \in P$ and t is odd, or $\gamma_1 \in Q$ and $t \equiv 2 \pmod 4$.

If $\gamma_1 \in P$, we use Table II to find γ_2:

$$\gamma_2 = \gamma_1 \cdot \beta^t / 2^t.$$

(Since t is odd, we do *not* have $\gamma_1 \sim \gamma_2$; note that $N(\gamma_2)$ will be odd.) Now compute γ_3, using Table IV:

$$\gamma_3 \equiv \gamma_2 \times (111) \pmod 4.$$

Then $2\gamma_1 \times \beta^{t+1}/2^{t+1} \sim \gamma_3$, where γ_3 is reduced, and we use Table V to find m.

If $\gamma_1 \in Q$, we use the procedure described previously to find a $\gamma' \sim \gamma_1$ with $\gamma' \in P$, and then proceed as above.

Example (a). Let $\gamma = 5 + 7\alpha + 4\alpha^2$. Then $\gamma \equiv (130) \pmod 4$, $\gamma \in P$, γ is not reduced. We find $N(\gamma) = 388 = 4 \cdot 97$, so we know: $\gamma \cdot (111)/2$ is reduced and $\gamma \cdot (111)^2/4$ must have odd norm, congruent to 1 (mod 4). This gives the sequence

$$130 \to 101 \sim 3 \cdot (110) \to 3 \cdot (010).$$

Since (030) is not in Table V, a match for this is $\beta^2 = 2^2$. Since (030) has odd norm, we have $2^6 \| m$.

Example (b). Let $\gamma = 9 + 5\alpha + 3\alpha^2$. Then $N(\gamma) = 4^5$, and we can use Table III. The sequence is (each arrow represents a single application of the multiplier (110))

$$113 \to 331 \to 113 \to 331 = 3 \cdot (113) \to 333.$$

We use here the fact that, in Table III, the entries (111), (133), (313) are all equivalent mod $\sim$. Then from Table V, $2^6 \| m$.

Example (c). Let $\gamma = 5 + 5\alpha + 3\alpha^2$: $N(\gamma) = 2^4 \cdot 17$. We have

$$G = \begin{bmatrix} 5 & -3 & 1 \\ 5 & 5 & -3 \\ 3 & -1 & 7 \end{bmatrix}, \quad \operatorname{adj} G = 4 \begin{bmatrix} 8 & 5 & 1 \\ -11 & 8 & 5 \\ -5 & -1 & 10 \end{bmatrix}.$$

Then $(5, 5, 3) \cdot (8, -11, -5) = 4 \cdot 17$; since $17 \equiv 1 \pmod 4$,

$$(5, 5, 3) \sim 17 \cdot (8, -11, -5) \equiv (8, -11, -5) \equiv (0, 1, 3) \pmod 4.$$

Since $|\operatorname{adj} G| = |G|^2 = 2^8 \cdot 17^2$, we know that $N(8, -11, -5) = 4 \cdot 17^2$. Then from Table II,

$$013 \sim 112 \to 321 \sim 3 \cdot (132) \to 3 \cdot (032).$$

Then $\gamma \sim \gamma'$, where $\gamma' \equiv (012) \pmod 4$. From Table V, $2^2 \| m$.

Example (d). Let $\gamma_1 = 8 + 3\alpha + \alpha^2$, $\gamma = 2\gamma_1$. We find $N(\gamma_1) = 2^5 \times 13$, and we have the sequence:

$$(031) \sim 3 \times (112) \to 3 \times (130) \to 3 \times (112)$$
$$\to 3 \times (130) \to (303) \to (232) \sim (120).$$

Here, $\gamma_1 \equiv (031)$ and $\gamma_2 \equiv (232)$. Then $\gamma_3 \equiv (111) \times (120) = (333)$. From Table V, $2^6 \| m$.

Appendix 1

Let $Z = 8y + 1$, and $\omega = (1 + \sqrt{Z})/2$. We denote $n + m\omega$ by (n, m); in all these tables, n, m are reduced modulo 4. R is the set of integers in $Q(\sqrt{Z})$. Tables Ia and Ib give the multiplication in $R/(4)$, for the two cases y even and y odd, for values of $(n, m) \not\equiv (0, 0) \pmod 2$. Table II gives $N(n + m\omega)$, reduced modulo 4. For Table III: given $(n, m) \not\equiv (0, 0) \pmod 2$, where $N(n + m\omega)$ is even. Choose β in R so that $N(\beta) = 2b$, $b \equiv 1 \pmod 4$ and $\beta \cdot (n + m\omega) = 2(a + b\omega)$. Write $N(n + m\omega) = 2^j x$, x odd. Then Table III gives the values of (a, b) modulo 4. For Table IV, we have $X = 2(n + m\omega)$ where $N(n + m\omega) = 2x$, x odd. Choose β as for Table III; $X \cdot \beta^2 = 4(a + b\omega)$; we give the values of $(a, b) \pmod 4$.

TABLE Ia (y even)

	10	20	30	01	11	21	31	02	12	22	32	03	13	23	33
10	10	20	30	01	11	21	31	02	12	22	32	03	13	23	33
20		00	20	02	22	02	22	00	20	00	20	02	22	02	22
30			10	03	33	23	13	02	32	22	12	01	31	21	11
01				01	02	03	00	02	03	00	01	03	00	01	02
11					13	20	31	00	11	22	33	02	13	20	31
21						01	22	02	23	00	21	01	22	03	20
31							13	00	31	22	13	00	31	22	13
02								00	02	00	02	02	00	02	00
12									10	22	30	01	13	21	33
22										00	22	00	22	00	22
32											10	03	31	23	11
03												01	00	03	02
13													13	22	31
23														01	20
33															13

TABLE Ib (y odd)

	10	20	30	01	11	21	31	02	12	22	32	03	13	23	33
10	10	20	30	01	11	21	31	02	12	22	32	03	13	23	33
20		00	20	02	22	02	22	00	20	00	20	02	22	02	22
30			10	03	33	23	13	02	32	22	12	01	31	21	11
01				21	22	23	20	02	03	00	01	23	20	21	22
11					33	00	11	00	11	22	33	22	33	00	11
21						21	02	02	23	00	21	21	02	23	00
31							33	00	31	22	13	20	11	02	33
02								00	02	00	02	02	00	02	00
12									10	22	30	01	13	21	33
22										00	22	00	22	00	22
32											10	03	31	23	11
03												21	20	23	22
13													33	02	11
23														21	00
33															33

TABLE II

$Z = 8y + 1$

$N(n + m\omega) \equiv r \pmod 4$, (n, m) reduced mod 4, not both even.

(n, m)	r (y even)	r (y odd)
(1, 1)	2	0
(3, 3)	2	0
(1, 3)	0	2
(3, 1)	0	2
(2, 1)	2	0
(2, 3)	2	0
(0, 1)	0	2
(0, 3)	0	2
(1, 0)	1	1
(3, 0)	1	1
(1, 2)	3	3
(3, 2)	3	3

TABLE III

y even					
$j > 1$			$j = 1$		
(n, m)	$j = 2$	$j > 2$	(n, m)	$X \equiv 1(4)$	$X \equiv 3(4)$
(1, 3)	(3, 3)	(3, 1)	(1, 1)	(3, 0)	(3, 2)
(3, 1)	(1, 1)	(1, 3)	(3, 3)	(1, 0)	(1, 2)
(0, 1)	(2, 3)	(0, 1)	(2, 1)	(3, 0)	(1, 2)
(0, 3)	(2, 1)	(0, 3)	(2, 3)	(1, 0)	(3, 2)

y odd					
$j > 1$			$j = 1$		
(n, m)	$j = 2$	$j > 2$	(n, m)	$X \equiv 1(4)$	$X \equiv 3(4)$
(1, 1)	(3, 1)	(3, 3)	(1, 3)	(1, 0)	(1, 2)
(3, 3)	(1, 3)	(1, 1)	(3, 1)	(3, 0)	(3, 2)
(2, 1)	(0, 3)	(2, 1)	(0, 1)	(3, 0)	(1, 2)
(2, 3)	(0, 1)	(2, 3)	(0, 3)	(1, 0)	(3, 2)

TABLE IV

For these tables: $U = 2(n + m\omega)$ where $N(n + m\omega) = 2x$, x odd. Let $\beta = \omega + 2$ if y is even, n and m odd; $\beta = \omega + 1$ if y is even, n even, m odd; $\beta = \omega$ if y is odd, n and m odd; and $\beta = \omega - 1$ if y is odd, n even, m odd. Then $(\beta^2/4)U = a + b\omega$.

y even			
$x \equiv 1 \pmod 4$		$x \equiv 3 \pmod 4$	
$1(n, m)$	(a, b)	(n, m)	(a, b)
(1, 1)	(2, 3)	(1, 1)	(2, 1)
(3, 3)	(2, 1)	(3, 3)	(2, 3)
(2, 1)	(3, 3)	(2, 1)	(1, 1)
(2, 3)	(1, 1)	(2, 3)	(3, 3)

y odd			
$x \equiv 1 \pmod 4$		$x \equiv 3 \pmod 4$	
(n, m)	(a, b)	(n, m)	(a, b)
(1, 3)	(0, 1)	(1, 3)	(0, 3)
(3, 1)	(0, 3)	(3, 1)	(0, 1)
(0, 1)	(1, 3)	(0, 1)	(3, 1)
(0, 3)	(3, 1)	(0, 3)	(1, 3)

TABLE V

(a) $Z \equiv 2 \pmod 4$

n	m		Exact power of 2 dividing disc S
odd	even	$n + m \equiv 1 \pmod 4$	2^6
odd	even	$n + m \equiv 3 \pmod 4$	2^8
odd	odd		2^{10}
even	odd		2^{11}

(b) $Z \equiv 3 \pmod 4$

n	m	Exact power of 2 dividing disc S
odd	$4j$	2^4
odd	$4j + 2$	2^6
even	odd	2^8
odd	odd	2^9

(c) $Z \equiv 5 \pmod{16}$

n	m		Exact power of 2 dividing disc S
$4k + 1$	$4j$		$2 \nmid$ disc S
$4k + 1$	$4j + 1$		
$4k + 2$	$4j + 3$		
all others with n, m not both even			2^4
$2k$	$2j$	j, k not both even	2^6

(d) $Z \equiv 13 \pmod{16}$

n	m		Exact power of 2 dividing disc S
$4k + 1$	$4j$		
$4k + 3$	$4j + 1$		$2 \nmid$ disc S
$4k$	$4j + 3$		
all others with n, m not both even			2^4
$2k$	$2j$	j, k not both even	2^6

(e) $Z = 8y + 1$

n	m	Exact power of 2 dividing disc S
$4k + 1$	$4j$	$2 \nmid$ disc S
$4k + 3$	$4j + 2$	2^2
$4k + 1$	$4j + 2$	2^2
$4k + 3$	$4j$	2^4
$2k$	$4j + 1$ (k–y odd)	2^5
$2k + 1$	$4j + 3$ (k–y odd)	2^5
$2k$	$4j + 1$ (k–y even)	2^3
$2k + 1$	$4j + 3$ (k–y even)	2^3
$4k + 2$	$4j$	2^6

Appendix 2

TABLE I

For this table, $(2) = P_1P_2P_3$ in R, $U = \{e\}$, $a \sim P_1^2$, $b \sim P_2^2$, $f \sim P_3^2$, $c \sim P_2^2P_3^2$, $g \sim P_1^2P_2^2$, $d \sim P_1^2P_3^2$.

	e	a	b	c	d	f	g	0
e	e	a	b	c	d	f	g	0
a		a	g	0	d	d	g	0
b			b	c	0	c	g	0
c				c	0	c	0	0
d					d	d	0	0
f						f	0	0
g							g	0
0								0

TABLE II

For this table, $(2) = PQ$ in R where Q has degree 2.

Then $U = \{e, a, b\}$; $f, c, d \sim P^2$ and $g \sim Q^2$.

	e	a	b	c	d	f	g	0
e	e	a	b	c	d	f	g	0
a		b	e	f	c	d	g	0
b			a	d	f	c	g	0
c				d	f	c	0	0
d					c	d	0	0
f						f	0	0
g							g	0
0								0

TABLE III

For this table, $(2) = PQ^2$ in R; $U = \{e, g\}$, $a \sim Q^2$, $b \sim Q^4$, $c, d \sim P^2$, $f \sim P^2Q^2$.

	e	a	b	c	d	f	g	0
e	e	a	b	c	d	f	g	0
a		b	b	f	f	0	a	0
b			b	0	0	0	b	0
c				d	c	f	d	0
d					d	f	c	0
f						0	f	0
g							e	0
0								0

TABLE IV

For this table, $(2) = P^3$ in R; $U = \{e, c, d, g\}$; $a, f \sim P^2$ and $b \sim P^4$.

	e	a	b	c	d	f	g	0
e	e	a	b	c	d	f	g	0
a		b	0	f	a	b	f	0
b			0	b	b	0	b	0
c				d	g	a	e	0
d					e	f	c	0
f						b	a	0
g							d	0
0								0

Appendix 3

TABLE I

The first column is $\beta = (abc)$; the second column is $\beta \cdot (010)^2$, the third is $\beta \cdot (010)^4$, the last column gives $N(\beta)$ modulo 4. All entries are given modulo 4.

β	$\beta\alpha^2$	$\beta\alpha^4$	$N(\beta)$
100	001	230	1
102	021	030	1
120	201	232	1
122	221	032	1
110	303	213	2
112	323	013	0
130	103	211	0
132	123	011	2
111	133	313	0
131	333	311	0
113	113	113	0

TABLE II

$\beta \cdot (111)/2 = (xyz)$

β	xyz
110	010, 232
112	103, 321
130	323, 101
132	012, 230

TABLE III

$\beta \cdot (110)/2 = (xyz)$

β	xyz
111	010, 032, 212, 230
131	021, 003, 223, 201
113	111, 133, 313, 331

TABLE IV

$\times$	110	112	130	132	111	131	113
102	312	310	332	330	333	313	331
120	132	130	112	110	333	313	331
122	330	332	310	312	111	131	113

TABLE V

We list those γ (modulo 4) such that (a) γ is reduced relative to 2, and (b) γ has a match β^2 with $\beta \not\equiv 0 \pmod 2$. For each γ we give the corresponding β, and the power of 2 dividing $N(\beta^2\gamma)$.

γ	β	$N(\beta^2\gamma)$
100, 001, 230	1	odd
213, 110, 303	(110)	2^3
322, 223, 012		2^2
131, 333, 311	(111)	2^6
122, 221, 032, 320, 203, 212, 010, 023, 302	(111)	2^4

If γ is reduced and not listed above, then a match for γ is $\beta^2 = 2^2$.

Department of Mathematics
University of North Carolina at Greensboro
Greensboro, North Carolina 27412

1. DANIEL A. MARCUS, *Number Fields*, Springer-Verlag, New York, 1977.
2. DANIEL SHANKS, "Dihedral quartic approximations and series for π", *J. Number Theory*, v. 14, 1982, pp. 397–423.
3. THERESA P. VAUGHAN, *On Computing the Discriminant of an Algebraic Number Field*. (Preprint.)