ACTA ARITHMETICA
177.4 (2017)

Some real quadratic number fields whose Hilbert 2-class fields have class number congruent to 2 modulo 4

by

Elliot Benjamin (Rindge, NH) and C. Snyder (Orono, ME)

1. Introduction. Let k be a real quadratic number field. It is well known that k has infinite 2-class field tower when the rank of its 2-class group $\mathrm{Cl}_2(k)$ is greater than 5, thanks to Golod and Shafarevich [6]. However, if the rank is between 2 and 5, there is no known decision procedure for determining whether or not k has infinite 2-class field tower. It is known, though, by group theory [3], that when the 2-rank of the class group of the Hilbert 2-class field k^1 of a number field k is ≤ 2, the 2-class field tower of k is finite (of length at most 3).

If we are interested in developing a decision procedure for determining precisely when the 2-class field tower of a number field k is infinite, then we could start by sieving out some of those fields where we know the tower is finite, namely, number fields k with $\operatorname{rank}\mathrm{Cl}_2(k^1) \leq 2$. In the case of real quadratic number fields we have already started this project in [2], in a fairly modest way, by determining all real quadratic fields k for which k^1 has odd class number, (and hence the 2-class field tower has length ≤ 1).

In this note, we determine when a real quadratic field k with discriminant d_k a sum of two squares has 2-class number of k^1, $h_2(k^1)$, equal to 2.

For imaginary quadratic number fields k, in [1] we have already determined when $\mathrm{Cl}_2(k^1)$ is cyclic. This is now our first major goal for real quadratic fields k. If $\mathrm{Cl}_2(k)$ is cyclic, then group theory tells us that $h_2(k^1) = 1$. Moreover, if the rank of $\mathrm{Cl}_2(k)$ is ≥ 4, then the theory of central class fields implies that the rank of $\mathrm{Cl}_2(k^1)$ is ≥ 2 (hence $\mathrm{Cl}_2(k^1)$ is not cyclic)—see, e.g., [1]. This leaves only the rank 2 and 3 cases. When the rank is 2, we have reduced the problem to a purely group-theoretical result about finite metabelian

2010 *Mathematics Subject Classification*: Primary 11R29; Secondary 20D15.
Key words and phrases: real quadratic fields, Hilbert class field, 2-class groups, metabelian 2-groups.
Received 30 March 2016; revised 26 August 2016.
Published online 6 March 2017.

DOI: 10.4064/aa8485-9-2016

2-groups G with two generators. For our applications, $G = \mathrm{Gal}(k^2/k)$, where k^2 is the 2-class field of k^1. The characterization of cyclic $\mathrm{Cl}_2(k^1)$ is equivalent to determining when the commutator subgroup G' of G is cyclic. This naturally splits into two cases (assuming G' is non-trivial): when the order of G' is 2, and when it is > 2. In the first case, we only need to consider at worst the order of the abelianization of the Frattini subgroup of G. This translates into determining the 2-class number of the genus class field, k_{gen}, of k. The second case, however, may involve the order of the abelianization of other normal subgroups of index 4 in G as well. In terms of number fields, it requires knowing the 2-class number of certain D_4-extensions of $\mathbb{Q}$, as well as that of k_{gen}. This is why we are starting with the determination of when $h_2(k^1) = 2$, as a first step.

Our restriction to discriminants that are a sum of two squares simplifies our proofs in some nontrivial ways. We leave the remaining case open for now.

2. Some properties of finite metabelian 2-groups. Let G be a finite metabelian 2-group generated by two or three elements. We will be interested in coming up with useful conditions which imply that the commutator subgroup G' of G has order 1 or 2.

We will start by recalling some "commutator calculus" and other relevant facts. Assume for the moment G is an arbitrary group written multiplicatively. If $x, y \in G$, then define as usual $[x, y] = x^{-1}y^{-1}xy$, the commutator of x with y. More generally, since $[*, *]$ is not associative, we define (inductively on n) $[x_1, \ldots, x_n] = [[x_1, \ldots, x_{n-1}], x_n]$ for all $x_j \in G$ and $n > 2$. If A and B are nonempty subsets of G, then $[A, B] = \langle\{[a, b] : a \in A, b \in B\}\rangle$. In particular the commutator subgroup G' is defined as $[G, G]$; also $G'' = (G')'$. Recall, too, that a group G is metabelian if $G'' = 1$, i.e., G' is abelian.

Of particular use is the lower central series $\{G_\ell\}$ of G, which is defined inductively as

$$G_1 = G \quad \text{and} \quad G_{\ell+1} = [G, G_\ell] \quad \text{for all } \ell \geq 1.$$

In particular, $G_2 = G'$. The lower central series is especially useful when the group G is nilpotent, i.e., the lower central series terminates in finitely many steps at the identity subgroup 1. As is well known, all finite p-groups (groups of p-power order) are nilpotent, for p any prime.

Now recall the following commutator identities [4]: for any $x, y, z \in G$,

$$[xy, z] = [x, z][x, z, y][y, z], \qquad [x, yz] = [x, z][x, y][x, y, z].$$

Of course when G is metabelian, the order of the factors above is immaterial; in addition if $z \in G'$, then

$$[z, x, y] = [z, y, x],$$

again when $G'' = 1$.

Now assume G is a finite metabelian p-group (p prime) and generated by two elements, say a and b. We introduce some more notation (cf. [4]): Let

$$\gamma_{1,1} = \gamma_{11} = [a, b],$$
$$\gamma_{r,s} = \gamma_{rs} = [a, b, x_1, \ldots, x_n] \quad \text{for } r, s \in \mathbb{N},$$

with $x_j = a$ or b, $n = r + s - 2$, and where r, resp. s, is the number of occurrences of a, resp. b, in the commutator. By the previous identity, γ_{rs} is independent of the order of the $x_1, \ldots, x_n$. For example,

$$\gamma_{11} = [a, b],$$
$$\gamma_{12} = [a, b, b], \quad \gamma_{21} = [a, b, a],$$
$$\gamma_{13} = [a, b, b, b], \quad \gamma_{22} = [a, b, a, b] = [a, b, b, a], \quad \gamma_{31} = [a, b, a, a].$$

It is known [4, Lemma 1.1] that for any $n \geq 2$,

$$G_n = \langle \{\gamma_{rs} : r, s \in \mathbb{N},\ r + s = n\}, G_{n+1} \rangle;$$

in particular,

$$G' = G_2 = \langle \gamma_{11}, G_3 \rangle, \quad G_3 = \langle \gamma_{12}, \gamma_{21}, G_4 \rangle.$$

Now we will consider the case where the 2-group G has two generators. Let G be a metabelian 2-group with $G^{\mathrm{ab}} = G/G' \simeq (2^m, 2^n)$ with $m, n \geq 1$. Let $G = \langle a, b \rangle$ be such that $a^{2^m} \equiv b^{2^n} \equiv 1 \bmod G'$. (These elements exist by the Burnside Basis Theorem [8].) Moreover, we let

$$H_1 = \langle a, b^2, G' \rangle, \quad H_2 = \langle ab, b^2, G' \rangle, \quad H_3 = \langle a^2, b, G' \rangle,$$

which are the three maximal subgroups of G. Finally, let J be the *Frattini subgroup* of G, i.e., the intersection of the maximal subgroups. Then

$$J = \langle a^2, b^2, G' \rangle.$$

Now, by the commutator identities above we see that

$$[a, b^2] \equiv [ab, b^2] \equiv [a^2, b] \equiv \gamma_{11}^2 \bmod G_3;$$

therefore

$$H_j' G_3 = \langle \gamma_{11}^2, G_3 \rangle = G_2^2 G_3.$$

Similarly, we find that $J' G_4 = G_2^4 G_3^2 G_4$. (Here G^m denotes the subgroup of G generated by the mth powers of the elements of G.)

Proposition 1. *Let G be a finite noncyclic metabelian 2-group with two generators, say a and b, and let H_j for $j = 1, 2, 3$ and J be as presented above. Then*

(i) $|G'| = 1$ *if and only if* $(G' : H_j') = 1$ *for some* (*equivalently, all*) $j \in \{1, 2, 3\}$;
(ii) $|G'| = 2$ *if and only if* $(G' : J') = 2$.

Proof. Consider (i). If $G' = 1$, then clearly $(G' : H'_j) = 1$ for each j. Conversely, if $|G'| > 1$, then by nilpotency $G_2 \neq G_3$, and hence $G_2 = \langle \gamma_{11}, G_3 \rangle \neq \langle \gamma_{11}^2, G_3 \rangle = G_2^2 G_3$. Notice that $H'_j \subseteq G_2^2 G_3$. Hence $(G' : H'_j) \neq 1$ for each j [2, Proposition 7].

For (ii), notice that if $|G'| = 2$, then clearly $(G' : J') = 2$, since in this case $J' \subseteq G_3 = 1$. Conversely, suppose $|G'| \neq 2$. If $G' = 1$ then all is clear. Hence suppose that $|G'| \geq 4$. Then we consider two cases.

Case 1: $(G_2 : G_3) \geq 4$. Notice that $J' \subseteq G_2^4 G_3$, and hence $(G_2 : J') \geq (G_2 : G_2^4 G_3) = 4$.

Case 2: $(G_2 : G_3) = 2$. This time $J' \subseteq G_4$. Now if $(G_3 : G_4) = 1$, then $G_3 = G_4$, which implies G_3 is trivial; but then $|G_2| = 2$, contrary to our assumption. Hence $(G_3 : G_4) \geq 2$, which in turn implies that

$$(G' : J') \geq (G_2 : G_4) = (G_2 : G_3)(G_3 : G_4) \geq 4. \blacksquare$$

We now convert Proposition 1 into statements about number fields. First recall a little notation, some of which we have seen already: If k is a number field, then $\mathrm{Cl}_2(k)$ is its 2-class group in the ordinary sense, $h_2(k)$ is the order of $\mathrm{Cl}_2(k)$, k^1 denotes the Hilbert 2-class field of k, and k^2 the 2-class field of k^1. If $G = \mathrm{Gal}(k^2/k)$, then as is well known by class field theory, $G' = \mathrm{Gal}(k^2/k^1) \simeq \mathrm{Cl}_2(k^1)$ and $G^{\mathrm{ab}} = G/G' \simeq \mathrm{Gal}(k^1/k) \simeq \mathrm{Cl}_2(k)$. Also, let (m, n) denote the direct sum of two cyclic groups of orders m and n. Finally, $(2^m)^*$ will denote any power of 2 divisible by 2^m.

Suppose that $\mathrm{Cl}_2(k) \simeq (2^*, 2^*)$. Then we let k_1, k_2, k_3 be the three quadratic extensions of k in k^1. Also let $K_g = k_1 k_2 k_3$ be the composite of the k_j.

Theorem 1. *Let k be a number field with 2-class group of rank 2 and let K_g be the maximal elementary abelian unramified 2-extension of k. Then the following four statements are equivalent:*

- (a_1) $h_2(k^1) = 1$;
- (a_2) *at least one of the three unramified quadratic extensions k_j of k satisfies $h_2(k_j) = h_2(k)/2$;*
- (a_3) *all three extensions k_j of k satisfy $h_2(k_j) = h_2(k)/2$;*
- (a_4) $h_2(K_g) = h_2(k)/4$.

Moreover, the following two statements, $(b_1), (b_2)$, are equivalent:

- (b_1) $h_2(k^1) = 2$;
- (b_2) $h_2(K_g) = h_2(k)/2$.

Finally, if $h_2(K_g) = h_2(k)/2$, then $h_2(k_j) = h_2(k)$ for all $j = 1, 2, 3$.

The content of Theorem 1(a_1)–(a_3) can be found in [2, Proposition 7].

Now we consider our 2-group G generated by three elements. Then we have the following simple result.

PROPOSITION 2. *Let G be a finite 2-group with three generators such that its commutator subgroup has order 2. Then there exists a maximal subgroup H in G such that $H' = G'$, and therefore $(H : H') = (G : G')/2$.*

Proof. Let $G = \langle a_1, a_2, a_3\rangle$. Furthermore, $G' = \langle c_{12}, c_{13}, c_{23}, G_3\rangle$ with $c_{ij} = [a_i, a_j]$. Now by assumption, G' has order 2. Without loss of generality, assume $G' = \langle c_{12}\rangle$. Then the maximal subgroup $H = \langle a_1, a_2, a_3^2, G'\rangle$ has $H' = G'$. Therefore, $(H : H') = (G : G')/2$. ∎

Converting this to number fields, we get

COROLLARY 1. *Let k be a number field with $\mathrm{Cl}_2(k)$ of rank 3 and suppose that $h_2(k^1) = 2$. Then there exists an unramified quadratic extension K of k such that $h_2(K) = h_2(k)/2$.*

3. Applications to some real quadratic fields. In this section we will apply our group-theoretic results, namely Theorem 1 and Corollary 1, to certain real quadratic fields.

Before starting, however, we isolate some results in the form of propositions that we will make use of.

PROPOSITION 3 (Kuroda's class number formula, [10]). *Let K/k be a normal quartic extension of number fields with Galois group of type $(2, 2)$, and let k_j $(j = 1, 2, 3)$ denote the quadratic subextensions. Then the class number of K satisfies*

$$h(K) = 2^{d-\kappa-2-v} q(K/k) h(k_1) h(k_2) h(k_3)/h(k)^2,$$

where $q(K/k) = (E_K : E_1E_2E_3)$ denotes the unit index of K/k (with $E_j = E_{k_j}$ the unit group of k_j), d is the number of infinite primes in k that ramify in K/k, κ is the $\mathbb{Z}$-rank of the unit group E_k of k, and $v = 0$ except when $K \subseteq k(\sqrt{E_k})$, in which case $v = 1$.

We may replace $h(\cdot)$ by $h_2(\cdot)$ in the proposition, since the unit index is a power of 2 (see [9]).

PROPOSITION 4. *Let $k = \mathbb{Q}(\sqrt{m})$ be a real quadratic number field with m a square-free integer. Suppose that the fundamental unit, $\varepsilon = \varepsilon_k$, of k has norm $+1$. Then there exists a principal ideal $\mathfrak{a} = (\alpha)$ different from the ideals (1) and $(\sqrt{m})$ which is a product of distinct ramified prime ideals.*

Moreover, $k(\sqrt{\varepsilon}) = k(\sqrt{\delta})$ for $\delta = \delta(\varepsilon) = N(\alpha_0) = N_{k/\mathbb{Q}}(\alpha_0)$, where $\alpha_0^{1-\sigma} = \varepsilon$ with σ denoting the nontrivial automorphism on k. (By cancelling all rational factors in (α_0) we get (α).) Notice that we may take $\alpha_0 = 1 + \varepsilon$ and thus also may take δ to be the square-free kernel of $N(1 + \varepsilon)$. Finally, $\chi_j(\delta) = +1$ for all genus characters χ_j of k.

See [2, Proposition 3 and its proof].

The following lemma and a special case of the subsequent proposition along with their proofs were shown to us by Franz Lemmermeyer in private communication for the case of odd discriminant.

LEMMA 1. *Let k be a real quadratic number field with discriminant d_k and fundamental unit ε_k. Suppose $N\varepsilon_k = -1$ and hence $d_k = 8^\nu p_1 \cdots p_t$ for primes $p_j \equiv 1 \bmod 4$ and $\nu = 0$ or 1. Then there exist $\mu_0 \in \mathbb{Z}[i]$, $\mu_0 \equiv 1 \bmod (2)$, $N\mu_0 = p_1 \cdots p_t$ and $\pi = 1+i$ or $1-i$ such that if $\mu = \pi^\nu \mu_0$, then $\mu\varepsilon_k$ is a square in $k(i)$.*

Proof. First suppose $\nu = 1$. Let $m = 2m_0$ with $m_0 = p_1 \cdots p_t$. We have $\varepsilon_k = x + y\sqrt{m}$ for some integers x, y. Since $N\varepsilon_k = -1$, we see $-1 = N\varepsilon_k = x^2 - my^2$, and therefore

$$(*) \qquad my^2 = x^2 + 1 = (x+i)(x-i).$$

Notice that since m is even, x is odd; moreover, since $m \equiv 2 \bmod 8$, y is odd. Next, observe that

$$2\mathbb{Z}[i] = (2) \subsetneq (x+i, x-i) \subseteq (1),$$

and so $(x+i, x-i) = (1+i)$ or (1). But since m is even, $(1+i) \mid (x \pm i)$, and hence $(x+i, x-i) = (1+i)$. By $(*)$ we have $x+i = \pi\mu_0\alpha^2$ and $x-i = \overline{\pi}\,\overline{\mu}_0\,\overline{\alpha}^2$, where $\pi = 1 \pm i$, $\mu_0\overline{\mu}_0 = m_0$, and $\alpha\overline{\alpha} = y$. We choose the sign of $1 \pm i$ as follows: If $x \equiv 1 \bmod 4$, let $\pi = 1 - i$. For $x \equiv 3 \bmod 4$, let $\pi = 1 + i$. The reason for choosing π thus is that in both cases $(x+i)/\pi \equiv i \bmod (2)$. Since $\alpha^2 \equiv 1 \bmod (2)$, we see $\mu_0 \equiv i \bmod (2)$. Now let $\mu = \pi\mu_0$ and set

$$\eta = \frac{1}{1+i}(\alpha\sqrt{\mu} + \overline{\alpha}\sqrt{\overline{\mu}}\,)$$

(where we take the principal branch of the square root). Hence $i\eta^2 = \varepsilon_k$. Multiplying this last equality by μ yields $\mu\varepsilon_k = i(\sqrt{\mu}\,\eta)^2$. But now

$$\sqrt{\mu}\,\eta = \frac{1}{1+i}(\alpha\mu + \overline{\alpha}\sqrt{m}) \in k(i).$$

Replacing μ by $i\mu$ then yields the desired result.

Now suppose $\nu = 0$. Then by replacing ε_k by ε_k^3 if necessary, we have a unit ε in $\mathbb{Z}[\sqrt{m_0}\,]$ with $N\varepsilon = -1$. Now the proof proceeds in the same way as before (but a little more easily, as $\gcd(x+i, x-i) = 1$ this time) and is left to the reader. ∎

PROPOSITION 5. *Let k be a real quadratic number field with discriminant d_k and fundamental unit ε_k. Suppose $N\varepsilon_k = -1$ and thus $d_k = d_1 \cdots d_t$ for positive prime discriminants d_j. Further suppose that $d_k = D_1 \cdots D_\ell$ where the D_j are coprime discriminants such that the fundamental units ε_j of the*

fields $\mathbb{Q}(\sqrt{D_j}\,)$ *all have norm* -1. *Then*

$$\sqrt{\varepsilon_1\varepsilon_2\cdots\varepsilon_\ell\varepsilon_k} \in k_{\rm gen}, \quad \textit{where} \quad k_{\rm gen} = \mathbb{Q}(\sqrt{d_1},\ldots,\sqrt{d_t}\,).$$

Proof. By Lemma 1 we have $\mu_1,\ldots,\mu_\ell$ and μ_k in $\mathbb{Z}[i]$ satisfying the congruence conditions of the lemma such that $\mu_j\varepsilon_j$ and $\mu_k\varepsilon_k$ are squares in $\mathbb{Q}(i,\sqrt{D_j}\,)$, resp., $k(i)$. Therefore

$$\mu_1\cdots\mu_\ell\mu_k\varepsilon_1\cdots\varepsilon_\ell\varepsilon_k$$

is a square in $k(i,\sqrt{D_1},\ldots,\sqrt{D_\ell}\,)$. But then $\mu_1\cdots\mu_\ell\mu_k$ is a product of squares in $\mathbb{Z}[i]$ and primes dividing d_k. Thus $\mu_1\cdots\mu_\ell\mu_k$ is a square in $k_{\rm gen}(i)$, and therefore $\varepsilon_1\cdots\varepsilon_\ell\varepsilon_k$ is a square in $k_{\rm gen}$. ∎

A special case of Propositions 4 and 5 is the following, which is used throughout some of the material below:

Corollary 2. *Let* d_1 *and* d_2 *be distinct positive prime discriminants and denote by* ε_1, ε_2, *and* ε_{12} *the fundamental units of* $\mathbb{Q}(\sqrt{d_1}\,)$, $\mathbb{Q}(\sqrt{d_2}\,)$, $\mathbb{Q}(\sqrt{d_1d_2}\,)$, *respectively. If* $N\varepsilon_{12}=+1$, *then* $\sqrt{\varepsilon_{12}} \in \mathbb{Q}(\sqrt{d_1},\sqrt{d_2}\,)$; *and if* $N\varepsilon_{12}=-1$, *then* $\sqrt{\varepsilon_1\varepsilon_2\varepsilon_{12}} \in \mathbb{Q}(\sqrt{d_1},\sqrt{d_2}\,)$.

Let k be a real quadratic number field with discriminant $d=d_k$ a sum of two integral squares. As noted above, $h_2(k^1)=2$ only when the rank of $\mathrm{Cl}_2(k)$ is 2 or 3. We consider these two cases separately. Since d_k is a sum of two squares, we have $d_k=d_1\cdots d_t$, where the d_j are positive prime discriminants. Moreover, recall that for d_k a sum of two squares, $\mathrm{Cl}_2(k)$ and $\mathrm{Cl}_2^+(k)$, the narrow 2-class group of k, both have the same rank which is equal to $t-1$.

$\mathrm{Cl}_2(k)$ **of rank 2.** Then $d=d_k=d_1d_2d_3$, where each d_j is >0 and is a prime discriminant. (Thus either d_j is a prime $\equiv 1 \bmod 4$, or $d_j=8$.) Let p_j denote the prime dividing d_j.

We consider further subcases:

$$\mathrm{Cl}_2^+(k)\simeq(2,2), \qquad \mathrm{Cl}_2^+(k)\simeq(2,4^*), \qquad \mathrm{Cl}_2^+(k)\simeq(4^*,4^*).$$

First consider $\mathrm{Cl}_2^+(k)\simeq(2,2)$. In this case $\mathrm{Gal}(k^2/k)$ is completely known [5], [2], and consequently so is $\mathrm{Cl}_2(k^1)$. Since the ranks of $\mathrm{Cl}_2(k)$ and $\mathrm{Cl}_2^+(k)$ are equal, we must have $\mathrm{Cl}_2(k)\simeq(2,2)$ and $N\varepsilon_k=-1$, where ε_k is the fundamental unit of k.

Here is some notation first. Let, for example, $h_2(d_1d_2)$ and $\varepsilon_{12}=\varepsilon_{d_1d_2}$ denote the 2-class number and fundamental unit of the field $\mathbb{Q}(\sqrt{d_1d_2}\,)$; $(d_1/d_2)=(d_1/p_2)$ denotes the Kronecker symbol; $(d_1/d_2)_4$ is the rational biquadratic residue symbol; and $(d/8)_4$ is defined as $+1$ for discriminants $d\equiv 1 \bmod 16$, and -1 for $d\equiv 9 \bmod 16$.

Theorem 2. *Let* k *be a real quadratic number field with discriminant* $d=d_k=d_1d_2d_3$, *where the* $d_j>0$ *are prime discriminants. Furthermore*

suppose $\mathrm{Cl}_2(k) \simeq \mathrm{Cl}_2^+(k) \simeq (2,2)$. *Then we have the following two possibilities: either*

(i) $(d_1/d_2) = (d_2/d_3) = (d_3/d_1) = -1$, *or*
(ii) (*without loss of generality*) $(d_1/d_2) = +1$ *and* $(d_1/d_3) = (d_2/d_3) = -1$.

Then $h_2(k^1) = 2$ *if and only if*

- *in case* (i), $(d_1d_2/d_3)_4(d_2d_3/d_1)_4(d_3d_1/d_2)_4 = -1$, *or equivalently*
$$\sqrt{\varepsilon_j\varepsilon_{d/d_j}\varepsilon_k} \in \mathbb{Q}(\sqrt{d_j}, \sqrt{d/d_j}\,) \quad \text{for } j = 1,2,3$$
(*here* $\mathrm{Gal}(k^2/k) \simeq H_8$, *the quaternion group of order* 8),
- *in case* (ii), *either*
(a) $(d_1/d_2)_4 = (d_2/d_1)_4 = -1$ *and* $\sqrt{\varepsilon_3\varepsilon_{12}\varepsilon_k} \notin \mathbb{Q}(\sqrt{d_3}, \sqrt{d_1d_2}\,)$, *or*
(b) $(d_1/d_2)_4 = (d_2/d_1)_4 = +1$ *and* $h_2(d_1d_2) = 4$
(*this time* $\mathrm{Gal}(k^2/k) \simeq D_4$, *the dihedral group of order* 8).

Proof. First, notice that $\mathrm{Cl}_2^+(k) \simeq (2,2)$ iff there are no C_4-splittings (splittings of the second kind) of d_k (see [12]). But this is true iff either (i) $(d_1/d_2) = (d_2/d_3) = (d_3/d_1) = -1$, or (ii) after possible reordering of the d_j, $(d_1/d_2) = +1$ and $(d_1/d_3) = (d_2/d_3) = -1$. Now, there are three unramified quadratic extensions of k, namely $k_j = k(\sqrt{d_j})$ for $j = 1,2,3$. By group theory [7], $\mathrm{Gal}(k^2/k)$ is either $(2,2)$, dihedral, quaternion, generalized quaternion, or semi-dihedral, and consequently $h_2(k^1) = \max\{h_2(k_j)/2 : j = 1,2,3\}$, and for $h_2(k^1) \neq 1$, we have $h_2(k_j) \geq 4$ for $j = 1,2,3$. Hence we obtain the following criterion:

$$h_2(k^1) = 2 \;\Leftrightarrow\; h_2(k_j) = 4 \ (j = 1,2,3).$$

We will compute $h_2(k_j)$ using Kuroda's class number formula:

$$h_2(k_j) = \tfrac{1}{4}q(k_j/\mathbb{Q})h_2(d_j)h_2(d/d_j)h_2(k) = q(k_j/\mathbb{Q})h_2(d/d_j),$$

where $q(k_j/\mathbb{Q}) = (E_j : e_{d_j}e_{d/d_j}e_k)$, where E_j and e_{d_j} etc. are the unit groups of k_j and $\mathbb{Q}(\sqrt{d_j}\,)$ etc.

First consider (i) above. Consider k_1; since $(d_2/d_3) = -1$ and so $h_2(d_2d_3) = 2$, we have $h_2(k_1) = h_2(d_2d_3)q(k_1/\mathbb{Q}) = 4$ iff $q(k_1/\mathbb{Q}) = 2$ iff $\sqrt{\varepsilon_1\varepsilon_{23}\varepsilon_k} \in k_1$ (see [9]), and similarly for k_j, $j = 2,3$. [5, Théorème 2] implies that $\mathrm{Gal}(k^2/k) \simeq H_8$ or $(2,2)$. By [2, Proposition 2], we then see that $\mathrm{Gal}(k^2/k) \simeq H_8$ iff $(d_1d_2/d_3)_4(d_2d_3/d_1)_4(d_3d_1/d_2)_4 = -1$.

Now consider (ii). First suppose $(d_1/d_2)_4 \neq (d_2/d_1)_4$. Then $h_2(d_1d_2) = 2$ and $N\varepsilon_{12} = +1$ (see [13], [11]). Hence $q(k_3/\mathbb{Q}) = 1$, since $\sqrt{\varepsilon_{12}}$ is the only candidate for a nontrivial square root in E_3, but this cannot happen [9]. Hence $h_2(k_3) = 2$, which implies $h_2(k^1) = 1$. Next, suppose $(d_1/d_2)_4 =$

$(d_2/d_1)_4 = -1$; then $h_2(d_1d_2) = 4$ and $N\varepsilon_{12} = -1$ again [13], [11]. We have

$$h_2(k_3) = 4q(k_3/\mathbb{Q}) = \begin{cases} 4 & \text{if } \sqrt{\varepsilon_3\varepsilon_{12}\varepsilon_k} \notin k_3, \\ 8 & \text{otherwise.} \end{cases}$$

Moreover, one can easily see that $h_2(k_1) = h_2(k_2) = 4$. Hence $h_2(k^1) = 2$ if and only if $\sqrt{\varepsilon_3\varepsilon_{12}\varepsilon_k} \notin k_3$. Finally, suppose $(d_1/d_2)_4 = (d_2/d_1)_4 = +1$. Then $h_2^+(d_1d_2) \geq 8$ (see [13], [11]). Now if $N\varepsilon_{12} = -1$, then $h_2(d_1d_2) \geq 8$, and so $h_2(k_3) \geq 8$. On the other hand, if $N\varepsilon_{12} = +1$, then $h_2(d_1d_2) \geq 4$, and so $h_2(k_3) \geq 4$. Also notice that $h_2(k_1) = h_2(k_2) = 4$. But in this case $h_2(k^1) = 2$ if and only if $h_2(k_3) = 4$ if and only if $h_2(d_1d_2) = 4$, since $N\varepsilon_{12} = +1$ and $q(k_3/\mathbb{Q}) = 1$. ∎

Next, we consider the case where $\mathrm{Cl}_2^+(k) \simeq (2^*, 4^*)$ and $N\varepsilon_k = -1$ (and thus $\mathrm{Cl}_2(k) \simeq (2^*, 4^*)$).

THEOREM 3. *Let k be a real quadratic number field with discriminant $d = d_k = d_1d_2d_3$, where the d_j are positive prime discriminants, and suppose that $\mathrm{Cl}_2(k) \simeq (2^*, 4^*)$. Further suppose $N\varepsilon_k = -1$. Then $h_2(k^1) \neq 2$.*

Proof. Assume to the contrary that $h_2(k^1) = 2$. Since $\mathrm{Cl}_2^+(k) \simeq (2^*, 4^*)$, we see by [12] that either (i) $(d_1/d_2) = (d_2/d_3) = (d_3/d_1) = +1$ (in which case $\mathrm{Cl}_2^+(k) \simeq (4^*, 4^*)$), or (ii) after possible reordering of the d_j, $(d_1/d_2) = -1$ and $(d_1/d_3) = (d_2/d_3) = +1$ (in which case $\mathrm{Cl}_2^+(k) \simeq (2, 4^*)$).

First consider (i). Let $k_j = k(\sqrt{d_j})$ for $j = 1, 2, 3$, and $K_g = k_1k_2k_3$. Notice that $K_g = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}, \sqrt{d_3}) = k_{\mathrm{gen}}$. By Theorem 1, we have

$$h_2(k^1) = 2 \quad \text{iff} \quad h_2(K_g) = h_2(k)/2,\ h_2(k_j) = h_2(k)\ (j = 1, 2, 3).$$

By Proposition 3, we see that

$$h_2(k_j) = \tfrac{1}{4}q(k_j/\mathbb{Q})h_2(k)h_2(d/d_j)h_2(d_j) \quad (j = 1, 2, 3),$$
$$h_2(K_g) = \tfrac{1}{8}q(K_g/k)h_2(k_1)h_2(k_2)h_2(k_3)/h_2(k)^2.$$

Putting all these together we see that $h_2(k^1) = 2$ if and only if

$$q(k_j/\mathbb{Q})h_2(d/d_j) = 4\ (j = 1, 2, 3) \quad \text{and} \quad q(K_g/k) = 4.$$

Since $(d_i/d_j) = +1$ for all $i \neq j$, we have $h_2^+(d/d_j) \geq 4$. Also notice that $h_2(d/d_j) \geq 2$, and thus when $h_2(d/d_j) = 2$ we have $N\varepsilon_{d/d_j} = +1$. Hence $q(k_j/\mathbb{Q})h_2(d/d_j) = 4$ if and only if either $q(k_j/\mathbb{Q}) = 1$ and $h_2(d/d_j) = 4$, or $q(k_j/\mathbb{Q}) = 2$ and $h_2(d/d_j) = 2$, in which case $N\varepsilon_{d/d_j} = +1$.

We claim that $q(k_j/\mathbb{Q}) = 1$ for each j. Suppose not; without loss of generality suppose $q(k_1/\mathbb{Q}) = 2$. Hence $h_2(d_2d_3) = 2$ and $N\varepsilon_{23} = +1$. But then we must have $\sqrt{\varepsilon_{23}} \in k_1$ (see [9]), which is impossible by Proposition 4, hence the claim. Therefore $h_2(d/d_j) = 4$ and $q(k_j/\mathbb{Q}) = 1$ for $j = 1, 2, 3$.

Hence $q(K_g/k) = (E_{K_g} : \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_{12}, \varepsilon_{13}, \varepsilon_{23}, \varepsilon_k\rangle)$. By our assumption the only possible units with positive norm are among $\varepsilon_{12}, \varepsilon_{13}, \varepsilon_{23}$. First

suppose all three have positive norms: $N\varepsilon_{ij} = +1$. Then all $\sqrt{\varepsilon_{ij}}$ are in K_g, implying that $q(K_g/k) \geq 8$.

Now suppose exactly two of these units have positive norms: say $N\varepsilon_{12} = -1$ and $N\varepsilon_{13} = N\varepsilon_{23} = +1$. Hence $\sqrt{\varepsilon_{13}}, \sqrt{\varepsilon_{23}} \in K_g$. Let $K = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_2}\,)$; then $\sqrt{\varepsilon_1\varepsilon_2\varepsilon_{12}} \in K$ by Proposition 5. But then $\sqrt{\varepsilon_1\varepsilon_2\varepsilon_{12}} \in K_g$, and once again we see $q(K_g/k) \geq 8$.

Next, suppose $N\varepsilon_{12} = N\varepsilon_{13} = -1$ and $N\varepsilon_{23} = +1$. Then the argument above shows $\sqrt{\varepsilon_{23}}, \sqrt{\varepsilon_1\varepsilon_2\varepsilon_{12}}, \sqrt{\varepsilon_1\varepsilon_3\varepsilon_{13}} \in K_g$, implying again $q(K_g/k) \geq 8$.

Finally, suppose $N\varepsilon_{ij} = -1$ for all i, j. Then $\sqrt{\varepsilon_i\varepsilon_j\varepsilon_{ij}} \in K_g$, and once again $q(K_g/k) \geq 8$.

All of this contradicts the assumption that $h_2(k^1) = 2$.

Now assume (ii) holds. As in the case of (i), we have $q(K_g/k) = 4$ and $q(k_j/\mathbb{Q})h_2(d/d_j) = 4$ $(j = 1, 2, 3)$. Since $(d_1/d_2) = -1$, we have $h_2(d_1d_2) = 2$ and $N\varepsilon_{12} = -1$. Hence $q(k_3/\mathbb{Q}) = 2$, and so $E_3 = \langle -1, \varepsilon_3, \varepsilon_{12}, \sqrt{\varepsilon_3\varepsilon_{12}\varepsilon_k}\,\rangle$. Now we consider cases depending on the size of $h_2(d_1d_3)$ and $h_2(d_2d_3)$.

Case 1: $h_2(d_1d_3)$ or $h_2(d_2d_3)$ is 2, say $h_2(d_1d_3) = 2$. This implies from the above that $q(k_2/\mathbb{Q}) = 2$. Since $(d_1/d_3) = +1$, we have $h_2^+(d_1d_3) \geq 4$ and so $N\varepsilon_{13} = +1$. But $E_2 = \langle -1, \varepsilon_2, \varepsilon_{13}, \varepsilon_k\,\rangle$, a contradiction. Therefore, Case 1 cannot occur (given that $h_2(k^1) = 2$).

Case 2: $h_2(d_1d_3) = h_2(d_2d_3) = 4$. Thus $q(k_2/\mathbb{Q}) = q(k_1/\mathbb{Q}) = 1$, and so

$$E_1E_2E_3 = \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_{12}, \varepsilon_{13}, \varepsilon_{23}, \sqrt{\varepsilon_3\varepsilon_{12}\varepsilon_k}\,\rangle.$$

But then $E_{K_g} \supseteq \langle \sqrt{\varepsilon_{13}^*}, \sqrt{\varepsilon_{23}^*}, \sqrt{\varepsilon_1\varepsilon_2\varepsilon_{12}}, E_1E_2E_3\,\rangle$, where

$$\varepsilon_{ij}^* = \begin{cases} \varepsilon_{ij} & \text{if } N\varepsilon_{ij} = +1, \\ \varepsilon_i\varepsilon_j\varepsilon_{ij} & \text{if } N\varepsilon_{ij} = -1. \end{cases}$$

Therefore $q(K_g/k) \geq 8$, and so this case cannot occur either. ∎

Now we consider what happens when $N\varepsilon_k = +1$.

Theorem 4. *Let k be a real quadratic number field with discriminant $d = d_k = d_1d_2d_3$, where the d_j are positive prime discriminants. Further suppose $N\varepsilon_k = +1$ and that either*

(i) $(d_1/d_2) = (d_2/d_3) = (d_3/d_1) = +1$ (*hence* $\mathrm{Cl}_2^+(k) \simeq (4^*, 4^*)$), *or*
(ii) (*after possible reordering of the* d_j) $(d_1/d_2) = -1$ *and* $(d_1/d_3) = (d_2/d_3) = +1$ (*thus* $\mathrm{Cl}_2^+(k) \simeq (2, 4^*)$).

Then $h_2(k^1) = 2$ if and only if either

(a) $h_2(d_1d_2) = h_2(d_1d_3) = h_2(d_2d_3) = 2$, *or*
(b) (*after possible reordering of the* d_j) $h_2(d_1d_2) = h_2(d_1d_3) = 2$, $h_2(d_2d_3) = 4$, $N\varepsilon_{23} = -1$, *and when* (i) *holds,* $\delta(\varepsilon_k)$ *is not a square in* $k(\sqrt{d_1})$.

Proof. First assume (i) holds.

Suppose $h_2(k^1) = 2$. We have $q(K_g/k) = 4$ and either $q(k_j/\mathbb{Q}) = 1$ and $h_2(d/d_j) = 4$, or $q(k_j/\mathbb{Q}) = 2$ and $h_2(d/d_j) = 2$, for $j = 1, 2, 3$. Since $N\varepsilon_k = +1$ we see $k(\sqrt{\varepsilon_k})/k$ is unramified by Proposition 5, and hence without loss of generality $k(\sqrt{\varepsilon_k}) = k_3 = \mathbb{Q}(\sqrt{d_3}, \sqrt{d_1 d_2})$. Hence $\delta(\varepsilon_k) \in \{p_3, p_1p_2\}$ and $E_3 = E_{k_3} = \langle -1, \varepsilon_3, \varepsilon_{12}, \sqrt{\varepsilon_k}\rangle$. Consequently, $q(k_3/\mathbb{Q}) = 2$ and $h_2(d_1d_2) = 2$, and thus $N\varepsilon_{12} = +1$. We now consider three cases depending on the signs of $N\varepsilon_{13}$ and $N\varepsilon_{23}$.

Case 1: $N\varepsilon_{13} = N\varepsilon_{23} = -1$. Then $q(k_1/\mathbb{Q}) = q(k_2/\mathbb{Q}) = 1$; more precisely, $E_1 = \langle -1, \varepsilon_1, \varepsilon_{23}, \varepsilon_k\rangle$ and $E_2 = \langle -1, \varepsilon_2, \varepsilon_{13}, \varepsilon_k\rangle$. Hence

$$E_1E_2E_3 = \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_{12}, \varepsilon_{13}, \varepsilon_{23}, \sqrt{\varepsilon_k}\rangle.$$

But since $\sqrt{\varepsilon_{12}}, \sqrt{\varepsilon_1\varepsilon_3\varepsilon_{13}}, \sqrt{\varepsilon_2\varepsilon_3\varepsilon_{23}} \in K_g$ (by Propositions 4 and 5), we see $q(K_g/k) \geq 8$. Therefore, this case cannot occur.

Case 2: $N\varepsilon_{13} \neq N\varepsilon_{23}$, say $N\varepsilon_{13} = +1$, $N\varepsilon_{23} = -1$. Hence $q(k_1/\mathbb{Q}) = 1$ and so $h_2(d_2d_3) = 4$. Moreover, since $\delta(\varepsilon_{13}) \in \{p_1, p_3\}$, we have $\delta(\varepsilon_{13})\delta(\varepsilon_k)$ in k_2^2, the squares of k_2, and therefore $\sqrt{\varepsilon_{13}\varepsilon_k} \in E_2$. This implies that $q(k_2/\mathbb{Q}) = 2$, and so $h_2(d_1d_3) = 2$. Also notice that $\delta(\varepsilon_k) \notin k_1^2$.

Case 3: $N\varepsilon_{13} = N\varepsilon_{23} = +1$. Then arguing as in the previous case we see $\sqrt{\varepsilon_{13}\varepsilon_k} \in k_2$ and $\sqrt{\varepsilon_{23}\varepsilon_k} \in k_1$, and thus $q(k_1/\mathbb{Q}) = q(k_2/\mathbb{Q}) = 2$. Therefore, $h_2(d_1d_3) = h_2(d_2d_3) = 2$ (along with $h_2(d_1d_2) = 2$ from the above).

Conversely, assume (a), i.e., $h_2(d_id_j) = 2$ for each $i \neq j$. By Theorem 1, if we can show $h_2(K_g) = h_2(k)/2$, then we can conclude that $h_2(k^1) = 2$ in this case. We will start by showing $h_2(k_j) = h_2(k)$ for each j, and then use this to get a handle on $h_2(K_g)$ by Kuroda's class number formula, i.e., Proposition 3. Toward this end, first notice that since $(d_i/d_j) = +1$ for all $i \neq j$, and $h_2(d_id_j) = 2$, we must have $h_2^+(d_id_j) = 4$, and so $N\varepsilon_{ij} = +1$ for all $i \neq j$. Now since $N\varepsilon_k = +1$, we see as before, without loss of generality, that $k(\sqrt{\varepsilon_k}) = k_3$. Hence $q(k_3/\mathbb{Q}) = 2$, since $E_3 = \langle -1, \varepsilon_3, \varepsilon_{12}, \sqrt{\varepsilon_k}\rangle$. By the Kuroda class number formula we thus have

$$h_2(k_3) = \tfrac{1}{4}q(k_3/\mathbb{Q})h_2(d_3)h_2(d_1d_2)h_2(k) = h_2(k).$$

Also notice that, as argued above, $E_1 = \langle -1, \varepsilon_1, \varepsilon_{23}, \sqrt{\varepsilon_{23}\varepsilon_k}\rangle$ and $E_2 = \langle -1, \varepsilon_2, \varepsilon_{13}, \sqrt{\varepsilon_{13}\varepsilon_k}\rangle$, which gives $q(k_1/\mathbb{Q}) = q(k_2/\mathbb{Q}) = 2$. Therefore by Kuroda's class number formula we have $h_2(k_1) = h_2(k_2) = h_2(k)$.

From this we see

$$h_2(K_g) = \tfrac{1}{8}q(K_g/k)h_2(k_1)h_2(k_2)h_2(k_3)/h_2(k)^2 = \tfrac{1}{8}q(K_g/k)h_2(k).$$

We will be done with this case if we can show $q(K_g/k) = 4$. First notice that by Theorem 1, since $h_2(k^1) \neq 1$, we have $h_2(K_g) \geq h_2(k)/2$, which implies that $q(K_g/k) \geq 4$. We will actually construct the unit group of K_g explicitly.

Since

$$E_1E_2E_3 = \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_{12}, \sqrt{\varepsilon_{13}}, \sqrt{\varepsilon_{23}}, \sqrt{\varepsilon_k}\rangle$$

and any unit in K_g must be a square root of an element of $E_1E_2E_3$ (see [14]), for example, we will use this observation to reduce the work required to determine E_{K_g}. We are reduced to considering units of K_g that are square roots of units η of the form $\eta = \varepsilon_1^{a_1}\varepsilon_2^{a_2}\varepsilon_3^{a_3}\varepsilon_{12}^{a_4}\sqrt{\varepsilon_{13}^{a_5}\varepsilon_{23}^{a_6}\varepsilon_k^{a_7}}$ for some $a_j \in \{0,1\}$. But if η is a square in E_{K_g}, then the norm $N_{K_g/k_j}\eta$ must be a square in E_j for each $j = 1,2,3$. This means we will need to see how the Galois group $G = \mathrm{Gal}(K_g/\mathbb{Q})$ acts on all the units $\varepsilon_j, \sqrt{\varepsilon_{ij}}, \sqrt{\varepsilon_k}$. Notice that $G = \langle \sigma_1, \sigma_2, \sigma_3\rangle$ where $\sigma_i(\sqrt{d_i}) = -\sqrt{d_i}$ and $\sigma_i(\sqrt{d_j}) = \sqrt{d_j}$ for $j \neq i$. Thus the fields k_1, k_2, k_3 are fixed fields of the subgroups generated by $\sigma_2\sigma_3, \sigma_1\sigma_3, \sigma_1\sigma_2$, respectively. Here is a table of these units and some of their conjugates and relative norms, where $\nu_j \in \{0,1\}$.

η	η^{σ_1}	η^{σ_2}	η^{σ_3}	$\eta^{1+\sigma_1\sigma_2}$	$\eta^{1+\sigma_1\sigma_3}$	$\eta^{1+\sigma_2\sigma_3}$
ε_1	$-1/\varepsilon_1$	ε_1	ε_1	-1	-1	ε_1^2
ε_2	ε_2	$-1/\varepsilon_2$	ε_2	-1	ε_2^2	-1
ε_3	ε_3	ε_3	$-1/\varepsilon_3$	ε_3^2	-1	-1
ε_{12}	$1/\varepsilon_{12}$	$1/\varepsilon_{12}$	ε_{12}	ε_{12}^2	1	1
$\sqrt{\varepsilon_{13}}$	$(-1)^{\nu_2}/\sqrt{\varepsilon_{13}}$	$\sqrt{\varepsilon_{13}}$	$(-1)^{\nu_2+1}/\sqrt{\varepsilon_{13}}$	$(-1)^{\nu_2}$	$-\varepsilon_{13}$	$(-1)^{\nu_2+1}$
$\sqrt{\varepsilon_{23}}$	$\sqrt{\varepsilon_{23}}$	$(-1)^{\nu_3}/\sqrt{\varepsilon_{23}}$	$(-1)^{\nu_3+1}/\sqrt{\varepsilon_{23}}$	$(-1)^{\nu_3}$	$(-1)^{\nu_3+1}$	$-\varepsilon_{23}$
$\sqrt{\varepsilon_k}$	$(-1)^{\nu_4}/\sqrt{\varepsilon_k}$	$(-1)^{\nu_4}/\sqrt{\varepsilon_k}$	$(-1)^{\nu_4+1}/\sqrt{\varepsilon_k}$	ε_k	$-\varepsilon_k$	$-\varepsilon_k$

To see how the table is constructed, we will look at the units ε_1, $\sqrt{\varepsilon_{13}}$, and $\sqrt{\varepsilon_k}$. Notice that $\varepsilon_1^{\sigma_1} = \varepsilon_1'$ (the conjugate of ε_1 over $\mathbb{Q}$) and since $-1 = N\varepsilon_1 = \varepsilon_1\varepsilon_1'$, we have $\varepsilon_1' = -1/\varepsilon_1$. Clearly $\varepsilon_1^{\sigma_2} = \varepsilon_1^{\sigma_3} = \varepsilon_1$. Also $\varepsilon_2, \varepsilon_3$ are handled in the same way.

Next notice that $\mathbb{Q}(\sqrt{\varepsilon_{13}}) = \mathbb{Q}(\sqrt{d_1}, \sqrt{d_3})$, which is the fixed field of σ_2. Hence $\sqrt{\varepsilon_{13}}^{\sigma_2} = \sqrt{\varepsilon_{13}}$. On the other hand, $\varepsilon_{13}^{\sigma_1} = \varepsilon_{13}' = 1/\varepsilon_{13} = \varepsilon_{13}^{\sigma_3}$. Hence in particular $\sqrt{\varepsilon_{13}}^{\sigma_1} = \pm 1/\sqrt{\varepsilon_{13}}$. Set $\sqrt{\varepsilon_{13}}^{\sigma_1} = (-1)^{\nu_2}/\sqrt{\varepsilon_{13}}$. But then we must have $\sqrt{\varepsilon_{13}}^{\sigma_3} = -\sqrt{\varepsilon_{13}}^{\sigma_1}$, since otherwise $\sigma_1\sigma_3$ fixes $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_3})$, which is clearly not the case. The unit $\sqrt{\varepsilon_{23}}$ behaves in a similar way.

Finally, notice that $\mathbb{Q}(\sqrt{\varepsilon_k}) = k_3 = \mathbb{Q}(\sqrt{d_3}, \sqrt{d_1d_2})$, which is fixed by $\sigma_1\sigma_2$ but not by any of the σ_j. Hence for $j = 1,2,3$, $\varepsilon_k^{\sigma_j} = \varepsilon_k' = 1/\varepsilon_k$, and so in particular $\sqrt{\varepsilon_k}^{\sigma_1} = (-1)^{\nu_4}/\sqrt{\varepsilon_k}$ for $\nu_4 = 0$ or 1. Since $\sigma_1\sigma_2$ restricts to the identity on k_3, we see $\sqrt{\varepsilon_k}^{\sigma_2} = \sqrt{\varepsilon_k}^{\sigma_1}$. On the other hand, we must have $\sqrt{\varepsilon_k}^{\sigma_3} = -\sqrt{\varepsilon_k}^{\sigma_1}$, since otherwise $\sigma_1\sigma_3$ would fix k_3, which is not the case.

The last three columns give the norm of η from K_g to k_3, k_2, k_1, respectively.

Now consider once again $\eta = \varepsilon_1^{a_1}\varepsilon_2^{a_2}\varepsilon_3^{a_3}\varepsilon_{12}^{a_4}\sqrt{\varepsilon_{13}^{a_5}\varepsilon_{23}^{a_6}\varepsilon_k^{a_7}}$, and assume that η is a square in E_{K_g}. Then

$$\eta^{1+\sigma_1\sigma_2} = (-1)^{a_1+a_2}\varepsilon_3^{2a_3}\varepsilon_{12}^{2a_4}(-1)^{\nu_2 a_5+\nu_3 a_6}\varepsilon_k^{a_7}$$

must be a square in $E_3 = \langle -1, \varepsilon_3, \varepsilon_{12}, \sqrt{\varepsilon_k}\rangle$. Hence, as $\eta > 0$ (being a square), we must have

$$a_1 + a_2 + \nu_2 a_5 + \nu_3 a_6 \equiv 0 \bmod 2.$$

Next notice that

$$\eta^{1+\sigma_1\sigma_3} = (-1)^{a_1+a_3}\varepsilon_2^{2a_2}(-\varepsilon_{13})^{a_5}(-1)^{(\nu_3+1)a_6}(-\varepsilon_k)^{a_7}$$

is a square in $E_2 = \langle -1, \varepsilon_2, \varepsilon_{13}, \sqrt{\varepsilon_{13}\varepsilon_k}\rangle$. Hence

$$a_5 = a_7,$$

which we assume from now on. Also notice that

$$a_1 + a_3 + (\nu_3 + 1)a_6 \equiv 0 \bmod 2.$$

Finally,

$$\eta^{1+\sigma_2\sigma_3} = \varepsilon_1^{2a_1}(-1)^{a_2+a_3+(\nu_2+1)a_5}(-\varepsilon_{23})^{a_6}(-\varepsilon_k)^{a_5}$$

is a square in $E_1 = \langle -1, \varepsilon_1, \varepsilon_{23}, \sqrt{\varepsilon_{23}\varepsilon_k}\rangle$. Hence

$$a_6 = a_5, \quad \text{and} \quad a_2 + a_3 + (\nu_2 + 1)a_5 \equiv 0 \bmod 2.$$

Summarizing, we see that if $\eta \in K_g^2$, then in particular

$$\eta = \varepsilon_1^{a_1}\varepsilon_2^{a_2}\varepsilon_3^{a_3}\varepsilon_{12}^{a_4}\sqrt{\varepsilon_{13}\varepsilon_{23}\varepsilon_k}^{\,a}$$

with some $a_1, a_2, a_3, a_4, a \in \{0, 1\}$. Since we already know that $\sqrt{\varepsilon_{12}} \in E_{K_g}$, we will assume $a_4 = 0$. Notice that if $a = 0$, then $\eta = 1$, for otherwise some a_j equals 1, in which case $\eta^{\sigma_j} < 0$, which cannot happen. Thus if $\eta \neq 1$, we have $a = 1$. In this case we get the following congruences mod 2 among the a_j:

$$\begin{aligned} a_1 + a_2 &\equiv \nu_2 + \nu_3, \\ a_1 + a_3 &\equiv \nu_3 + 1, \\ a_2 + a_3 &\equiv \nu_2 + 1, \end{aligned}$$

which reduces to the two solutions

$$(a_1, a_2, a_3) \equiv (0, \nu_2 + \nu_3, \nu_3 + 1) + (\mu, \mu, \mu) \bmod 2, \qquad \mu = 0, 1.$$

Hence

$$\eta \equiv (\varepsilon_1\varepsilon_2\varepsilon_3)^{\mu}\varepsilon_2^{\nu_2+\nu_3}\varepsilon_3^{\nu_3+1}\sqrt{\varepsilon_{13}\varepsilon_{23}\varepsilon_k} \bmod (E_1E_2E_3)^2, \qquad \mu = 0, 1.$$

Note that both solutions cannot be in K_g^2, for otherwise $\varepsilon_1\varepsilon_2\varepsilon_3$ would be a square in K_g, which is not the case as we have just seen above. However, one of these η's is in K_g^2 since $q(K_g/k) \geq 4$. Hence $q(K_g/k) = 4$ and we even have

$$E_{K_g} = \left\langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3, \sqrt{\varepsilon_{12}}, \sqrt{\varepsilon_{13}}, \sqrt{\varepsilon_{23}}, \sqrt{(\varepsilon_1\varepsilon_2\varepsilon_3)^{\mu}\varepsilon_2^{\nu_2+\nu_3}\varepsilon_3^{\nu_3+1}\sqrt{\varepsilon_{13}\varepsilon_{23}\varepsilon_k}} \right\rangle,$$

for exactly one value of $\mu \in \{0, 1\}$.

Therefore $h_2(k^1) = 2$ when $h_2(d_1d_2) = h_2(d_1d_3) = h_2(d_2d_3) = 2$.

Now assume (b), i.e., $h_2(d_1d_2) = h_2(d_1d_3) = 2$, $h_2(d_2d_3) = 4$, $N\varepsilon_{23} = -1$, and $\delta(\varepsilon_k) \notin k_1^2$. Then $k(\sqrt{\varepsilon_k})$ is k_2 or k_3 (it cannot be k_1 since by assumption $\delta(\varepsilon_k)$ is not a square in k_1). Without loss of generality assume $\mathbb{Q}(\sqrt{\varepsilon_k}) = k_3$. Then $E_3 = \langle -1, \varepsilon_3, \varepsilon_{12}, \sqrt{\varepsilon_k}\rangle$, which implies $q(k_3/\mathbb{Q}) = 2$. Hence $h_2(k_3) = h_2(k)$ by Kuroda's class number formula. Next notice that $E_2 = \langle -1, \varepsilon_2, \varepsilon_{13}, \sqrt{\varepsilon_{13}\varepsilon_k}\rangle$, implying that $q(k_2/\mathbb{Q}) = 2$, and so $h_2(k_2) = h_2(k)$. Finally, $E_1 = \langle -1, \varepsilon_1, \varepsilon_{23}, \varepsilon_k\rangle$, which implies that $q(k_1/\mathbb{Q}) = 1$; and since $h_2(d_2d_3) = 4$, we still see that $h_2(k_1) = h_2(k)$.

As before, if we can show $q(K_g/k) = 4$, then we will be finished. Toward this end, notice that

$$E_1E_2E_3 = \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_{12}, \varepsilon_{23}, \sqrt{\varepsilon_{13}}, \sqrt{\varepsilon_k}\rangle.$$

Moreover, observe that $\sqrt{\varepsilon_{12}}, \sqrt{\varepsilon_2\varepsilon_3\varepsilon_{23}} \in E_{K_g}$, and so $q(K_g/k) \geq 4$. Hence we will be finished if we can show

$$E_{K_g} = \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3, \sqrt{\varepsilon_{12}}, \sqrt{\varepsilon_{13}}, \sqrt{\varepsilon_2\varepsilon_3\varepsilon_{23}}, \sqrt{\varepsilon_k}\rangle.$$

To see this, suppose

$$\eta = \varepsilon_1^{a_1}\varepsilon_2^{a_2}\varepsilon_3^{a_3}\varepsilon_{12}^{a_4}\varepsilon_{23}^{a_5}\sqrt{\varepsilon_{13}^{a_6}\varepsilon_k^{a_7}}$$

is a square in K_g. Then as before we see that its norms from K_g to k_3, k_2, k_1 must be squares in the corresponding unit groups E_3, E_2, E_1. Once again we need to consider the conjugates of the units as in the table above. All the rows are the same except that we will replace $\sqrt{\varepsilon_{23}}$ by simply ε_{23}, in which case we have

$$\varepsilon_{23}^{1+\sigma_1\sigma_2} = -1, \quad \varepsilon_{23}^{1+\sigma_1\sigma_3} = -1, \quad \varepsilon_{23}^{1+\sigma_2\sigma_3} = \varepsilon_{23}^2.$$

Now back to our η. Assume it is a square in E_{K_g}. Then

$$\eta^{1+\sigma_1\sigma_2} = (-1)^{a_1+a_2+a_5}\varepsilon_3^{2a_3}\varepsilon_{12}^{2a_4}(-1)^{\nu_2 a_6}\varepsilon_k^{a_7}$$

must be a square in $E_3 = \langle -1, \varepsilon_3, \varepsilon_{12}, \sqrt{\varepsilon_k}\rangle$. Therefore

$$a_1 + a_2 + a_5 + \nu_2 a_6 \equiv 0 \bmod 2.$$

Next

$$\eta^{1+\sigma_1\sigma_3} = (-1)^{a_1+a_3+a_5}\varepsilon_2^{2a_2}(-\varepsilon_{13})^{a_6}(-\varepsilon_k)^{a_7}$$

is a square in $E_2 = \langle -1, \varepsilon_2, \varepsilon_{13}, \sqrt{\varepsilon_{13}\varepsilon_k}\rangle$, and so

$$a_6 = a_7 \quad \text{and} \quad a_1 + a_3 + a_5 \equiv 0 \bmod 2.$$

Finally,

$$\eta^{1+\sigma_2\sigma_3} = \varepsilon_1^{2a_1}(-1)^{a_2+a_3}\varepsilon_{23}^{2a_5}(-1)^{(\nu_2+1)a_6}(-\varepsilon_k)^{a_6}$$

must be a square in $E_1 = \langle -1, \varepsilon_1, \varepsilon_{23}, \varepsilon_k\rangle$. Therefore,

$$a_6 = 0 \quad \text{and} \quad a_2 = a_3.$$

But notice that $a_5 \equiv a_1 + a_2 \bmod 2$, and thus

$$\eta = \varepsilon_1^{a_1}(\varepsilon_2\varepsilon_3)^{a_2}\varepsilon_{12}^{a_4}\varepsilon_{23}^{a_1+a_2+2\ell} = (\varepsilon_1\varepsilon_{23})^{a_1}(\varepsilon_2\varepsilon_3\varepsilon_{23})^{a_2}\varepsilon_{12}^{a_4}\varepsilon_{23}^{2\ell}.$$

We can see that $\varepsilon_2\varepsilon_3\varepsilon_{23}$ and ε_{12} are totally positive, but $(\varepsilon_1\varepsilon_{23})^{\sigma_1} < 0$. Hence $a_1 = 0$, and therefore

$$E_{K_g} = \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3, \sqrt{\varepsilon_{12}}, \sqrt{\varepsilon_2\varepsilon_3\varepsilon_{23}}, \sqrt{\varepsilon_{13}}, \sqrt{\varepsilon_k}\,\rangle,$$

as desired.

Now assume (ii).

First suppose $h_2(k^1) = 2$. Then $q(K_g/k) = 4$ and $q(k_j/\mathbb{Q})h_2(d/d_j) = 4$ for $j = 1, 2, 3$. But we must have $h_2(d_1d_2) = 2$ and $N\varepsilon_{12} = -1$, since $(d_1/d_2) = -1$. Hence $q(k_3/\mathbb{Q}) = 2$, and so $E_3 = \langle -1, \varepsilon_3, \varepsilon_{12}, \sqrt{\varepsilon_k}\,\rangle$. Now the argument is exactly as in (i) above. (The only change is that $k(\sqrt{\varepsilon_k}\,)$ is already determined to be k_3.)

Conversely, first assume (a). (Notice that $h_2(d_1d_2) = 2$ without any assumptions.) Again since $\chi_j(p_3) = +1$ for $j = 1, 2, 3$, we have $k(\sqrt{\varepsilon_k}\,) = k_3$. Arguing as in (i) above, we see

$$E_1E_2E_3 = \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_{12}, \sqrt{\varepsilon_{13}}, \sqrt{\varepsilon_{23}}, \sqrt{\varepsilon_k}\,\rangle.$$

Now, if $\eta \in E_1E_2E_3$ has its positive square root in E_{K_g}, then we find that $\eta = (\varepsilon_1\varepsilon_2\varepsilon_{12})^a(\varepsilon_1\varepsilon_2\varepsilon_3)^b(\varepsilon_1^{\nu_3+1}\varepsilon_2^{\nu_2+1}\sqrt{\varepsilon_{13}\varepsilon_{23}\varepsilon_k})^c$. The only change in the argument above is that now $N\varepsilon_{12} = -1$, and so $\varepsilon_{12}^{1+\sigma_1\sigma_2} = \varepsilon_{12}^2$, $\varepsilon_{12}^{1+\sigma_1\sigma_3} = -1$ and $\varepsilon_{12}^{1+\sigma_2\sigma_3} = -1$. We then obtain

$$E_{K_g} = \left\langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3, \sqrt{\varepsilon_1\varepsilon_2\varepsilon_{12}}, \sqrt{\varepsilon_{13}}, \sqrt{\varepsilon_{23}}, \sqrt{(\varepsilon_1\varepsilon_2\varepsilon_3)^\mu\varepsilon_1^{\nu_3+1}\varepsilon_2^{\nu_2+1}\sqrt{\varepsilon_{13}\varepsilon_{23}\varepsilon_k}}\right\rangle$$

for exactly one value of μ in $\{0, 1\}$. Therefore $q(K_g/k) = 4$.

Now assume (b). Once again by considering the genus characters we have $k(\sqrt{\varepsilon_k}\,) = k_3$. This time we find (as before)

$$E_1E_2E_3 = \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_{12}, \varepsilon_{23}, \sqrt{\varepsilon_{13}}, \sqrt{\varepsilon_k}\,\rangle.$$

We also find

$$E_{K_g} = \langle -1, \varepsilon_1, \varepsilon_2, \varepsilon_3, \sqrt{\varepsilon_1\varepsilon_2\varepsilon_{12}}, \sqrt{\varepsilon_2\varepsilon_3\varepsilon_{23}}, \sqrt{\varepsilon_{13}}, \sqrt{\varepsilon_k}\,\rangle$$

and once again $q(K_g/k) = 4$, as desired.

This completes the proof. ∎

$\mathrm{Cl}_2(k)$ **of rank 3.** This time $d = d_k = d_1d_2d_3d_4$ for positive prime discriminants d_j, $j = 1, 2, 3, 4$. We then have the following result.

THEOREM 5. *Let k be a real quadratic number field with discriminant $d = d_k = d_1d_2d_3d_4$ for positive prime discriminants d_j. Then $h_2(k^1) > 2$.*

Proof. We know by [2] that $h_2(k^1) \neq 1$. Let K be any unramified quadratic extension of k. Then $K/\mathbb{Q}$ is a V_4-extension, with quadratic sub-

fields F_1, F_2, k. The Kuroda class number formula implies that

$$h_2(K) = \tfrac{1}{4} q(K/\mathbb{Q}) h_2(F_1) h_2(F_2) h_2(k),$$

where $q(K/\mathbb{Q}) = (E_K : E_{F_1} E_{F_2} E_k)$. Then either (i) $F_1 = \mathbb{Q}(\sqrt{d_j})$ and $F_2 = \mathbb{Q}(\sqrt{d/d_j})$, in which case $h_2(F_2) \geq 4$, or (ii) $F_1 = \mathbb{Q}(\sqrt{d_i d_j})$ and $F_2 = \mathbb{Q}(\sqrt{d/d_i d_j})$, in which case both $h_2(F_1), h_2(F_2) \geq 2$. In both cases, $h_2(K) \geq h_2(k)$, and therefore by Corollary 1, $h_2(k^1) \neq 2$. ∎

Summary of the main results. We now consolidate into one theorem most of the results (or equivalent versions) that we have established.

THEOREM 6 (Main Theorem). *Let k be a real quadratic number field whose discriminant is a sum of two rational integral squares. Then $h_2(k^1) = 2$ if and only if $d_k = d_1 d_2 d_3$ for d_j positive prime discriminants satisfying one of the following conditions:*

$(\frac{d_1}{d_2})$	$(\frac{d_2}{d_3})$	$(\frac{d_3}{d_1})$	*Additional conditions*
-1	-1	-1	$(\frac{d_1 d_2}{d_3})_4 (\frac{d_2 d_3}{d_1})_4 (\frac{d_3 d_1}{d_2})_4 = -1$
-1	-1	$+1$	$(\frac{d_1}{d_3})_4 = (\frac{d_3}{d_1})_4 = +1$, $h_2(d_1 d_3) = 4$ *or* $(\frac{d_1}{d_3})_4 = (\frac{d_3}{d_1})_4 = -1$, $\sqrt{\varepsilon_2 \varepsilon_{13} \varepsilon_k} \notin \mathbb{Q}(\sqrt{d_2}, \sqrt{d_1 d_3})$
-1	$+1$	$+1$	$(\frac{d_1}{d_3})_4 (\frac{d_3}{d_1})_4 = (\frac{d_2}{d_3})_4 (\frac{d_3}{d_2})_4 = -1$, $N\varepsilon_k = +1$ *or* $(\frac{d_1}{d_3})_4 (\frac{d_3}{d_1})_4 = -1$, $(\frac{d_2}{d_3})_4 = (\frac{d_3}{d_2})_4 = -1, N\varepsilon_k = +1$
$+1$	$+1$	$+1$	$(\frac{d_i}{d_j})_4 (\frac{d_j}{d_i})_4 = -1$ $(i \neq j)$, $N\varepsilon_k = +1$ *or* $(\frac{d_1}{d_j})_4 (\frac{d_j}{d_1})_4 = -1$ $(j \neq 1), (\frac{d_2}{d_3})_4 = (\frac{d_3}{d_2})_4 = -1$, $\delta(\varepsilon_k)$ *is not a square in* $\mathbb{Q}(\sqrt{d_1}, \sqrt{d_2 d_3})$, $N\varepsilon_k = +1$

Examples. We now give two examples of fields satisfying conditions (a) and (b) of Theorem 4.

EXAMPLE 1. Let $k = \mathbb{Q}(\sqrt{19669})$. Then $d_k = d_1 d_2 d_3$, where $d_1 = 89$, $d_2 = 17$, $d_3 = 13$, $(d_1/d_3) = (d_2/d_3) = -(d_1/d_2) = +1$, $h_2(d_1 d_2) = h_2(d_1 d_3) = h_2(d_2 d_3) = 2$, and $N\varepsilon_k = +1$ where $\varepsilon_k = 37025 + 264\sqrt{19669}$. (We also have $\mathrm{Cl}_2(k) \simeq (2,4)$ and thus $\mathrm{Cl}_2^+(k) \simeq (2,8)$.) By Theorem 4(a), we conclude that $h_2(k^1) = 2$.

EXAMPLE 2. Let $k = \mathbb{Q}(\sqrt{4520953})$. This time $d_k = d_1 d_2 d_3$, where $d_1 = 197$, $d_2 = 433$, $d_3 = 53$, $(d_i/d_j) = +1$ for all $i \neq j$, $N\varepsilon_k = +1$, $h_2(d_1 d_2) = h_2(d_1 d_3) = 2$, $h_2(d_2 d_3) = 4$, and $N\varepsilon_{23} = -1$. (We will not write out the fundamental unit ε_k this time as its integer coefficients have over 120 digits.) (Also we have $\mathrm{Cl}_2(k) \simeq (2,4)$ and thus $\mathrm{Cl}_2^+(k) \simeq (4,4)$.) In order to conclude that $h_2(k^1) = 2$, we need to show that $\delta(\varepsilon_k)$ is not a square in

$k_1 = k(\sqrt{d_1}) = \mathbb{Q}(\sqrt{197}, \sqrt{433 \cdot 53}\,)$. But $\delta(\varepsilon_k) = 53$, which is not a square in k_1. Therefore $h_2(k^1) = 2$ by Theorem 4(b).

Acknowledgements. Some of the calculations needed in the examples, including 2-class numbers and fundamental units, were done using Keith Matthews' number theory website, which may be found at http://www.numbertheory.org.

We would like to thank Professor Matthews for taking time (from his grandfather duties) to help us out with calculating $\delta(\varepsilon_k)$ in Example 2.

Our very special thanks go to Franz Lemmermeyer for, among other things, suggesting Lemma 1 and a special case of Proposition 5 and their proofs; verifying that $h_2(k^1) = 2$ in the two examples above using Pari; and suggesting editorial changes to improve the presentation in this paper. Thank you, Franz!

Finally, we would also like to thank the referee for a very careful reading of the manuscript and making recommendations for its improvement.

References

[1] E. Benjamin, F. Lemmermeyer and C. Snyder, *Imaginary quadratic fields k with cyclic* $\mathrm{Cl}_2(k^1)$, J. Number Theory 67 (1997), 229–245.

[2] E. Benjamin, F. Lemmermeyer and C. Snyder, *Real quadratic fields with abelian 2-class field tower*, J. Number Theory 73 (1998), 182–194.

[3] N. Blackburn, *On prime-tower groups in which the derived group has two generators*, Proc. Cambridge Philos. Soc. 53 (1957), 19–27.

[4] N. Blackburn, *On prime-power groups with two generators*, Proc. Cambridge Philos. Soc. 54 (1958), 327–337.

[5] R. Couture et A. Derhem, *Un problème de capitulation*, C. R. Acad. Sci. Paris Sér. I 314 (1992), 785–788.

[6] E. S. Golod and I. R. Shafarevich, *Infinite class field towers of quadratic fields*, Izv. Akad. Nauk SSSR 28 (1964), 273–276 (in Russian); English transl.: Amer. Math. Soc. Transl. 48 (1965), 91–102.

[7] D. Gorenstein, *Finite Groups*, Harper and Row, New York, 1968.

[8] B. Huppert, *Endliche Gruppen I*, Springer, 1967.

[9] T. Kubota, *Über den bizyklisch biquadratischen Zahlkörper*, Nagoya Math. J. 10 (1956), 65–85.

[10] F. Lemmermeyer, *Kuroda's class number formula*, Acta Arith. 66 (1994), 245–260.

[11] F. Lemmermeyer, *Die Konstruktion von Klassenkörpern*, Diss. Univ. Heidelberg, 1995.

[12] L. Rédei und H. Reichardt, *Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers*, J. Reine Angew. Math. 170 (1934), 69–74.

[13] A. Scholz, *Über die Lösbarkeit der Gleichung* $t^2 - Du^2 = -4$, Math. Z. 39 (1934), 95–111.

[14] H. Wada, *On the class number and the unit group of certain algebraic number fields*, J. Fac. Sci. Univ. Tokyo 13 (1966), 201–209.

Elliot Benjamin
CALCampus//P.O.Box 132
Rindge, NH 03461, U.S.A.
E-mail: ben496@prexar.com

C. Snyder
Department of Mathematics and Statistics
University of Maine
Orono, ME 04469, U.S.A.
E-mail: wsnyder@maine.edu