ACTA ARITHMETICA
LXXX.3 (1997)

On the 2-primary part of K_2 of rings of integers in certain quadratic number fields

by

A. Vazzana (Ann Arbor, Mich.)

1. Introduction. For quadratic fields whose discriminant has few prime divisors, there are explicit formulas for the 4-rank of $K_2\mathcal{O}_E$. For quadratic fields whose discriminant has arbitrarily many prime divisors, the formulas are less explicit. In this paper we will study fields of the form $\mathbb{Q}(\sqrt{p_1\ldots p_k})$, where the primes p_i are all congruent to 1 mod 8. We will prove a theorem conjectured by Conner and Hurrelbrink which examines under what conditions the 4-rank of $K_2\mathcal{O}_E$ is zero for such fields. In the course of proving the theorem, we will see how the conditions can be easily computed.

Acknowledgements. I would like to thank J. S. Milne for his help in the writing of this paper and P. E. Conner and J. Hurrelbrink for their helpful suggestions.

2. Statement of theorem. The theorem, which was proved by Conner and Hurrelbrink for the case $k = 1$ and $k = 2$ in [CH2] and [CH4], is:

Theorem 2.1. *Let $E = \mathbb{Q}(\sqrt{p_1\ldots p_k})$ with distinct rational primes $p_i \equiv 1 \bmod 8$ for $i = 1,\ldots,k$ and $k \geq 1$. Then the 2-primary part of $K_2\mathcal{O}_E$ is elementary abelian if and only if*

(i) *the 2-primary part of the ideal class group $C(E)$ is elementary abelian and the norm of the fundamental unit of E is -1, and*
(ii) *an odd number of the primes $p_1,\ldots,p_k$ fail to be represented over $\mathbb{Z}$ by the quadratic form $x^2 + 32y^2$.*

The attack will be the same as in the $k = 2$ case. First we show, under the assumption $4\text{-rk}\,K_2\mathcal{O}_E = 0$, that (i) holds. Then we show, under the assumption (i) is true, that $4\text{-rk}\,K_2\mathcal{O}_E = 0$ is equivalent to (ii). Following the notation in [CH3]:

- S is the set of infinite and dyadic places of E,
- $M = E(\sqrt{-1})$,

- $G_E = \{\mathrm{cl}(b) \in E^*/E^{*2} : \mathrm{ord}_{\mathfrak{p}}(b) \equiv 0 \bmod 2 \text{ for all } \mathfrak{p} \notin S\}$,
- $H_E = \{\mathrm{cl}(b) \in G_E : b \in N_{M/E}(M^*)\}$.

We will make use of the maps χ, χ_1, and $\chi_2 : H_E \to C_S(E)/C_S(E)^2$ defined in the same paper, where $C_S(E)$ is the S-class group of E. We give a list of the properties of these maps which we will need. The key result relating χ to $K_2\mathcal{O}_E$ is:

$$\text{(2.2)} \qquad 4\text{-rk}\, K_2\mathcal{O}_E = 0 \quad \text{if and only if} \quad 2\text{-rk} \ker \chi = 1.$$

The three maps satisfy the relation

$$\text{(2.3)} \qquad \chi = \chi_1\chi_2.$$

For the purposes of computation, χ_1 and χ_2 tend to be easier to work with. Let $\mathcal{O}_S$ be the ring of S-integers of E. If the class of b is in H_E, we can write

$$b\mathcal{O}_S = B^2$$

for some $\mathcal{O}_S$ ideal B. By definition, we have

$$\text{(2.4)} \qquad \chi_1(\mathrm{cl}(b)) = B.$$

Here we are writing B to mean the class it represents in $C_S(E)/C_S(E)^2$. If b is an S-unit, then

$$\text{(2.5)} \qquad \chi_1(\mathrm{cl}(b)) = 1.$$

If b is the norm of an S-unit from M, or -1 is the norm of an S-unit from $E(\sqrt{b})$, then

$$\text{(2.6)} \qquad \chi_2(\mathrm{cl}(b)) = 1.$$

Details for all of these statements can be found in [CH3].

3. Part 1 of the proof. In this section we show that $4\text{-rk}\, K_2\mathcal{O}_E = 0$ implies condition (i) in Theorem 2.1.

PROPOSITION 3.1. *If* $4\text{-rk}\, K_2\mathcal{O}_E = 0$, *then* $4\text{-rk}\, C(E) = 0$.

Proof. By the Hasse norm theorem, -1 is a norm from E. From [CH1, 18.3], we have

$$2\text{-rk}\, C(E) = k - 1.$$

We will exhibit an elementary abelian subgroup of the 2-primary part of $C(E)$ which contains no nontrivial squares and show that it has 2-rank $k-1$. Let $\mathfrak{P}_1, \ldots, \mathfrak{P}_k$ be the primes lying over $p_1, \ldots, p_k$ in E. We will be examining the subgroup of $C(E)$ generated by the classes of $\mathfrak{P}_1, \ldots, \mathfrak{P}_{k-1}$. Certainly this subgroup is elementary abelian. For a nonempty subset I of $\{1, \ldots, k-1\}$, let

$$p_I = \prod_{i \in I} p_i \quad \text{and} \quad \mathfrak{P}_I = \prod_{i \in I} \mathfrak{P}_i.$$

These $\mathfrak{P}_I$ are the elements of our subgroup. We will first show that none of the $\mathfrak{P}_I$ are squares. Then, we show that they represent distinct elements of $C(E)$, and so $\mathfrak{P}_1,\ldots,\mathfrak{P}_{k-1}$ will form a basis of the $\mathbb{Z}/2\mathbb{Z}$ module they generate.

We make use of χ to show that no $\mathfrak{P}_I$ is a square. Since 2 is an S-unit and the image of $1+i$ under $N_{M/E}$, the class of 2 lies in H_E. Also, since 2 is an S-unit, $\chi_1(\mathrm{cl}(2)) = 1$ (by (2.5)) and since 2 is the norm of $1+i$, $\chi_2(\mathrm{cl}(2)) = 1$ (by (2.6)). So from (2.3) we conclude that the class of 2 is in the kernel of χ. Under the assumption that $4\text{-rk}\,K_2\mathcal{O}_E = 0$, (2.2) implies that the class of 2 generates the kernel of χ. Next we see how χ acts on the class of p_i. Clearly $\mathrm{cl}(p_i)$ is in G_E. Since $p_i \equiv 1 \bmod 4$, p_i is in $N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\mathbb{Q}(\sqrt{-1})^*)$, and so p_i is in $N_{M/E}(M^*)$. Hence, the class of p_i is in fact in H_E. Let ε_i be the fundamental unit of $\mathbb{Q}(\sqrt{p_i})$. Then by [CH1, 18.4bis], $N_{\mathbb{Q}(\sqrt{p_i})/\mathbb{Q}}(\varepsilon_i) = -1$ and so $N_{E(\sqrt{p_i})/E}(\varepsilon_i) = -1$. We apply (2.6) to get $\chi_2(\mathrm{cl}(p_i)) = 1$. From (2.4), $\chi_1(\mathrm{cl}(p_i)) = \mathfrak{P}_i$. Thus, for any nonempty subset I of $\{1,\ldots,k-1\}$, we have shown $p_I \in H_E$ and

$$\chi(\mathrm{cl}(p_I)) = \mathfrak{P}_I.$$

If $\mathfrak{P}_I$ were a square in $C(E)$, then it would be a square in $C_S(E)$, and so the class of p_I would be in the kernel of χ. This cannot happen since the square class of 2 generates the kernel of χ.

We have shown that $\mathfrak{P}_I$ is not a square. In particular, this means $\mathfrak{P}_I$ is not principal. Next we check that the $\mathfrak{P}_I$ represent distinct classes in $C(E)$. Let I_1 and I_2 be distinct nonempty subsets of $\{1,\ldots,k-1\}$. If $\mathfrak{P}_{I_1}$ and $\mathfrak{P}_{I_2}$ differ by a principal ideal, then $\mathfrak{P}_{I_1}\mathfrak{P}_{I_2}$ is principal. Let $I = \{I_1\cup I_2\}\backslash\{I_1\cap I_2\}$. Then

$$\mathfrak{P}_I = \mathfrak{P}_{I_1}\mathfrak{P}_{I_2}.$$

Since $I_1 \neq I_2$, I is a nonempty subset of $\{1,\ldots,k-1\}$. Hence, $\mathfrak{P}_I$ is not principal, and so $\mathfrak{P}_{I_1} \neq \mathfrak{P}_{I_2}$ in $C(E)$. Therefore $\mathfrak{P}_1,\ldots,\mathfrak{P}_{k-1}$ do in fact form a basis of the $\mathbb{Z}/2\mathbb{Z}$ module they generate. We have shown that this group has a 2-rank of $k-1$ and contains no nontrivial squares. It follows that this group is all of the 2-primary part of $C(E)$, and so the 4-rank of $C(E)$ is zero. ∎

Let $C_+(E)$ denote the narrow class group of E.

PROPOSITION 3.2. *Suppose* $4\text{-rk}\,K_2\mathcal{O}_E = 0$. *Then* $4\text{-rk}\,C(E) = 0$ *if and only if* $4\text{-rk}\,C_+(E) = 0$.

Proof. Let $\nu : C_+(E) \to C(E)$ be the projection map. The surjectivity of ν makes the backwards implication clear. For the other direction, suppose $\mathfrak{a}$ is a fractional ideal of E representing an element of order 4 in $C_+(E)$. The kernel of ν is killed by 2 so $\mathfrak{a}$ necessarily maps to an element of order 2 in $C(E)$. From the proof of Proposition 3.1, we know that the elements of order 2 in $C(E)$ are exactly the $\mathfrak{P}_I$. So we must have $\mathfrak{a} = x\mathfrak{P}_I$ for some set

I and some x in E. This means that $\mathfrak{a}^2 = x^2 p_I \mathcal{O}_E$. Thus $\mathfrak{a}^2$ is generated by a totally positive element of E, and so $\mathfrak{a}$ has order at most 2. ∎

Now we can finish off the first step of our proof.

PROPOSITION 3.3. *If* $4\text{-rk}\, C_+(E) = 0$, *then the norm of the fundamental unit in* E *is* -1.

P r o o f. Write C_2 for $\mathrm{Gal}(E/\mathbb{Q})$. Then

$$H^0(C_2, \mathcal{O}_E^*) = \mathbb{Z}^*/N_{E/\mathbb{Q}}(\mathcal{O}_E^*).$$

Thus the norm of the fundamental unit is -1 if and only if $H^0(C_2, \mathcal{O}_E^*)$ is trivial. With notation as in [CH1], we examine

$$i_0 : H^0(C_2, \mathcal{O}_E^*) \to R^0(E/\mathbb{Q}).$$

Recall that -1 is a norm from E. Applying [CH1, 18.1] and [CH1, 2.3], we may conclude that i_0 is the trivial map. On the other hand, from [CH1, 12.12] the kernel of i_0 is isomorphic to the subgroup of elements of $\ker \nu$ which are squares in the narrow class group. Since $4\text{-rk}\, C_+(E) = 0$, the narrow class group has no nontrivial squares. Thus i_0 is also injective and $H^0(C_2, \mathcal{O}_E^*)$ is trivial. ∎

Putting Propositions 3.1–3.3 together, we have shown that if $4\text{-rk}\, K_2\mathcal{O}_E = 0$, then $4\text{-rk}\, C(E) = 0$ and the norm of the fundamental unit is -1. This completes the first part of the proof.

R e m a r k 3.4. We have seen that if the 4-rank of the narrow class group is zero, then condition (i) from Theorem 2.1 holds. Later we will show that the converse is true. The condition $4\text{-rk}\, C_+(E) = 0$ can be computed by the examination of a certain graph. With our field E, we associate a graph Γ_E whose vertices are the p_i. The vertices p_i and p_j are linked by an edge if and only if $\left(\frac{p_i}{p_j}\right) = -1$. Since all of the primes are congruent to 1 mod 4, by quadratic reciprocity $\left(\frac{p_i}{p_j}\right) = \left(\frac{p_j}{p_i}\right)$, and so this makes sense. An *Eulerian vertex decomposition* (EVD) of Γ_E is an unordered pair $\{V_1, V_2\}$ of sets of vertices such that

(1) $V_1 \cap V_2 = \emptyset$ and $V_1 \cup V_2 = \{p_1, \ldots, p_k\}$, and

(2) every vertex in V_i is adjacent to an even number of vertices in V_j for $i \neq j$, $i, j = 1, 2$.

We always have the trivial EVD $\{\emptyset, \{p_1, \ldots, p_k\}\}$. The Rédei–Reichardt theorem [H, 2.6] tells us that this is the only EVD exactly when the 4-rank of the narrow class group of E is zero.

PROPOSITION 3.5. *If* $4\text{-rk}\, C(E) = 0$ *and the norm of the fundamental unit is* -1, *then* $\mathfrak{P}_1, \ldots, \mathfrak{P}_{k-1}$ *generate the* 2*-primary part of* $C(E)$ *and* $4\text{-rk}\, C_+(E) = 0$.

Proof. In light of the arguments of the last paragraph in the proof of Proposition 3.1, to prove that $\mathfrak{P}_1, \ldots, \mathfrak{P}_{k-1}$ generate the 2-primary part of $C(E)$, we only need to show that $\mathfrak{P}_I$ is not principal for a nonempty subset I of $\{1, \ldots, k-1\}$. Suppose $\mathfrak{P}_I$ is principal. Then by taking norms, we would find that either p_I or $-p_I$ is the norm of an element of E^*. Since -1 is a norm from E, this means that p_I would be a norm from E. Thus, p_I is a local norm, and so

$$(p_I, p_1 \ldots p_k)_p = 1$$

for all primes p of $\mathbb{Q}$. By taking $p = p_j$ for j not in I, we have

$$\prod_{i \in I} \left(\frac{p_i}{p_j}\right) = 1.$$

By taking $p = p_j$ for j in I, we have

$$\prod_{i \notin I} \left(\frac{p_i}{p_j}\right) = 1.$$

Thus $\{I, \{i \notin I\}\}$ is a nontrivial EVD. From the preceding remark, the existence of such an EVD means that $4\text{-rk}\, C_+(E) \neq 0$.

We will now see that $4\text{-rk}\, C_+(E) = 0$. Consider

$$\nu : C_+(E) \to C(E).$$

If $\mathfrak{a}$ is in the kernel of ν, then $\mathfrak{a} = x\mathcal{O}_E$ for some x in E^*, which we may take to be positive. Let ε be a positive fundamental unit of E. If x is not totally positive, then since ε has norm -1, εx will be totally positive. Hence $\mathfrak{a}$ represents the identity in $C_+(E)$, and so ν is an isomorphism. Since $4\text{-rk}\, C(E) = 0$, $4\text{-rk}\, C_+(E) = 0$. ■

We have now shown that condition (i) from Theorem 2.1 is equivalent to $4\text{-rk}\, C_+(E) = 0$, which in turn is equivalent to the statement that the only EVD of Γ_E is the trivial one. This makes determining whether or not condition (i) holds easier to compute.

In the proof of Proposition 3.1, we saw, under the assumption $4\text{-rk}\, K_2\mathcal{O}_E = 0$, that the 2-primary part of the class group is generated by the $\mathfrak{P}_i$. We used this to prove that the 4-rank of the class group is zero. Now, under the assumption that $4\text{-rk}\, C(E) = 0$ and the norm of the fundamental unit is -1, we have that same description of the 2-primary part of the class group. We will use this throughout the second part of the proof to show $4\text{-rk}\, K_2\mathcal{O}_E = 0$.

4. Part 2 of the proof. The proof can now be completed by rereading the proof of the $k = 2$ case and replacing p_1 and p_2 by $p_1, \ldots, p_k$. We work through this argument providing some additional details. It remains to show, under the hypothesis that condition (i) holds, that $4\text{-rk}\, K_2\mathcal{O}_E = 0$ is equivalent to condition (ii).

We begin by trying to compute H_E in order to determine the kernel of χ. By [CH3, 2.4], G_E has a 2-rank of $k+3$. By Dirichlet's unit theorem, the S-units contribute 4 generators. The remaining classes are generated by $p_1, \ldots, p_{k-1}$. Let G_E^+ be the subgroup of G_E consisting of classes represented by totally positive elements. A norm from M is a sum of squares in E, and so is necessarily totally positive. Hence, H_E is a subgroup of G_E^+. Let U_S denote the group of S-units of E. Then $-1, 2$, and ε generate 3 distinct classes in U_S/U_S^2. Choose a positive S-unit $\widetilde{\pi}$ to complete a basis for U_S/U_S^2. Assume now that ε has norm -1. Let σ be the generator for $\mathrm{Gal}(E/\mathbb{Q})$. If $\sigma(\widetilde{\pi}) < 0$, then set $\pi = \varepsilon\widetilde{\pi}$. Otherwise, set $\pi = \widetilde{\pi}$. Thus π is totally positive and $\{-1, 2, \varepsilon, \pi\}$ is a basis for U_S/U_S^2. Since $2, p_1, \ldots, p_{k-1}$ are all totally positive, G_E^+ is generated by $\pi, 2, p_1, \ldots, p_{k-1}$.

PROPOSITION 4.1. *Suppose* $4\text{-rk}\, C(E) = 0$ *and the norm of* ε *is* -1. *Then* $4\text{-rk}\, K_2\mathcal{O}_E = 0$ *if and only if* π *fails to be a norm from* M.

Proof. The 2-primary part of $C(E)$ maps onto the 2-primary part of $C_S(E)$. Since -1 and 2 are norms from E, by [CH3, 7.1], the 2-rank of $C_S(E)$ is $k-1$. Thus

$$C(E)/C(E)^2 \cong C_S(E)/C_S(E)^2.$$

If π is a norm from M, then $G_E^+ = H_E$, and so H_E has a 2-rank of $k+1$. Since $C_S(E)/C_S(E)^2$ has a 2-rank of $k-1$, the 2-rank of the kernel of χ is at least 2, and so by (2.2), $4\text{-rk}\, K_2\mathcal{O}_E \neq 0$.

On the other hand, if π fails to be a norm from M, then G_E is generated by 2, $p_1, \ldots, p_{k-1}$. From Proposition 3.5, for a nonempty subset I of $\{1, \ldots, k-1\}$, $\mathfrak{P}_I$ is not principal. Thus $\mathfrak{P}_I$ represents a nontrivial class in $C(E)/C(E)^2$, and hence a nontrivial class in $C_S(E)/C_S(E)^2$. Recall that $\chi(\mathrm{cl}(p_I)) = \mathfrak{P}_I$. This means that the kernel of χ is generated by the class of 2, and so by (2.2), the 4-rank of $K_2\mathcal{O}_E$ is zero. ∎

The following sequence of lemmas will connect the condition on π to condition (ii) in the statement of Theorem 2.1.

LEMMA 4.2. *Suppose* $4\text{-rk}\, C(E) = 0$ *and the norm of* ε *is* -1. *Let* D_1 *be a dyadic prime of* E. *Then* π *fails to be a norm from* M *if and only if* $(\pi, -1)_{D_1} = -1$.

Proof. By the Hasse norm theorem, π is a norm from M if and only if $(\pi, -1)_{\mathfrak{P}} = 1$ for every prime $\mathfrak{P}$ of E. Since π and -1 are S-units and π is totally positive, this can only fail to happen when $\mathfrak{P}$ is a dyadic prime. If D_1 and D_2 are the dyadic primes of E, then by reciprocity

$$(\pi, -1)_{D_1} = (\pi, -1)_{D_2}.$$

Thus, in order to check whether π is a norm from M or not, it is enough to check whether $(\pi,-1)_{D_1}$ is equal to 1 or not. ∎

LEMMA 4.3. *If* $4\text{-rk}\, C(E)=0$ *and the norm of* ε *is* -1, *then* $(\pi,-1)_{D_1} = (2,\varepsilon)_{D_1}$.

Proof. We know that π is divisible by a dyadic prime, which we may assume to be D_1. Let

$$\pi' = \pi 2^{-\mathrm{ord}_{D_2}(\pi)}.$$

Since $(2,-1)_{D_1}=1$, by the bilinearity of the Hilbert symbol we have

$$(\pi',-1)_{D_1} = (\pi,-1)_{D_1}.$$

By the definition of the Hilbert symbol, we have $(\pi',\sigma(\varepsilon))_{D_1} = (\sigma(\pi'),\varepsilon)_{D_2}$. Since we are assuming that the norm of ε is -1, it follows from bilinearity and the previous statement that

$$(\pi',-1)_{D_1} = (\pi',\varepsilon)_{D_1}(\sigma(\pi'),\varepsilon)_{D_2}.$$

Another application of bilinearity and reciprocity gives

$$(\pi',-1)_{D_1} = (\pi'\sigma(\pi'),\varepsilon)_{D_1}.$$

The ideal generated by π' is a power of D_1. Thus the ideal generated by $\pi'\sigma(\pi')$ is a power of the ideal generated by 2. Since $\pi'\sigma(\pi')$ and 2 are both positive rational numbers, we actually have $\pi'\sigma(\pi') = 2^r$ as elements of E for some integer r. We now have

$$(\pi',-1)_{D_1} = ((2,\varepsilon)_{D_1})^r.$$

It remains to show that r is odd. First we show that D_1 has odd order in the class group of E. Let s be the order of D_1 in $C(E)$. If s were even, then $D_1^{s/2}$ would have order 2, and so by Proposition 3.5, the class of $D_1^{s/2}$ in $C(E)$ would be represented by some $\mathfrak{P}_I$. This would give rise to an element x from E such that

$$xD_1^{s/2} = \mathfrak{P}_I.$$

On taking norms we see that $p_I/2^{s/2}$ is in $N_{E/\mathbb{Q}}(E^*)$. From the Hasse norm theorem and the fact that the primes are congruent to 1 mod 8, 2 is also a norm, and so p_I must also be a norm. As in the proof of Proposition 3.5, this will lead to a nontrivial EVD, meaning that $4\text{-rk}\, C_+(E)\neq 0$. In light of Proposition 3.5, we have a contradiction.

Choose a positive generator d for D_1^s. Since $\pi'\mathcal{O}_E = D_1^r$, r must divide s and $\pi' = \varepsilon^n d^{r/s}$ for some integer n. If r were even, then since s is odd, r/s would have to be even. Thus, $d^{r/s}$ is totally positive and so n must be even. However, since π represents a square class different from the ones represented by 1 and 2, it follows that π' is not a square. Thus r must be odd. ∎

Lemma 4.4. *Let $\mathfrak{D}$ be the prime of M lying over D_1. Then $(2,\varepsilon)_{D_1} = (1+i,\varepsilon)_{\mathfrak{D}}$.*

Proof. First, if $(1+i,\varepsilon)_{\mathfrak{D}} = 1$, then $1+i$ is in the image of the local norm map $N : M_{\mathfrak{D}}(\sqrt{\varepsilon}) \to M_{\mathfrak{D}}$ where $M_{\mathfrak{D}}$ is the local field of M at $\mathfrak{D}$. Thus 2 is in the image of the local norm map $N : M_{\mathfrak{D}}(\sqrt{\varepsilon}) \to E_{D_1}$, and therefore in the image of $N : E_{D_1}(\sqrt{\varepsilon}) \to E_{D_1}$. Hence $(2,\varepsilon)_{D_1} = 1$. Now consider the commutative diagram

$$\begin{tikzcd}
M_{\mathfrak{D}}^*/N(M_{\mathfrak{D}}(\sqrt{\varepsilon})^*) \arrow[r, "\mathrm{rec}"] \arrow[d, "\mathcal{N}"'] & \mathrm{Gal}(M_{\mathfrak{D}}(\sqrt{\varepsilon})/M_{\mathfrak{D}}) \arrow[d, "\mathrm{inc}"] \\
E_{D_1}^*/N(M_{\mathfrak{D}}(\sqrt{\varepsilon})^*) \arrow[r, "\mathrm{rec}"] & \mathrm{Gal}(M_{\mathfrak{D}}(\sqrt{\varepsilon})/E_{D_1})
\end{tikzcd}$$

where rec is the map induced by the local Artin map, $\mathcal{N}$ is the map induced by the norm map, and inc is the inclusion map. Since the rec maps are isomorphisms, $\mathcal{N}$ is necessarily injective. We know that 2 is in the image of the local norm map $N : M_{\mathfrak{D}} \to E_{D_1}$. If 2 is also in the image of $N : E_{D_1}(\sqrt{\varepsilon}) \to E_{D_1}$, then by local class field theory, it is also in the image of $N : M_{\mathfrak{D}}(\sqrt{\varepsilon}) \to E_{D_1}$. Since $N_{M_{\mathfrak{D}}/E_{D_1}}(1+i) = 2$, $1+i$ is the kernel of the left vertical map. Hence, $1+i$ is in the image of $N : M_{\mathfrak{D}}(\sqrt{\varepsilon}) \to M_{\mathfrak{D}}$. ∎

The next lemma will allow us to translate the condition into a statement about $\mathbb{Q}(\sqrt{-1})$.

Lemma 4.5. *Suppose the norm of ε is -1. Then there exists an element $\delta \in \mathbb{Q}(\sqrt{-1})$ such that*

(1) $\delta \equiv \varepsilon \bmod M^{*2}$, *and*
(2) $N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\delta) \equiv p_1 \dots p_k \bmod \mathbb{Q}^{*2}$.

Proof. Recall that σ is the generator of $\mathrm{Gal}(E/\mathbb{Q})$. The condition that $N_{E/\mathbb{Q}}(\varepsilon) = -1$ can be rewritten as

$$\varepsilon\sigma(\varepsilon) = -1.$$

We will also use σ to mean the element of $\mathrm{Gal}(M/\mathbb{Q})$ which fixes $\mathbb{Q}(\sqrt{-1})$ and acts as the generator of $\mathrm{Gal}(E/\mathbb{Q})$ on E. Let τ be the element of $\mathrm{Gal}(M/\mathbb{Q})$ which fixes E and acts as the generator of $\mathrm{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q})$ on $\mathbb{Q}(\sqrt{-1})$. We have

$$N_{M/\mathbb{Q}(\sqrt{-1})}(i\varepsilon) = (i\varepsilon)\sigma(i\varepsilon).$$

Since σ fixes i, and $\varepsilon\sigma(\varepsilon) = -1$, we have

$$N_{M/\mathbb{Q}(\sqrt{-1})}(i\varepsilon) = 1.$$

Thus, by Hilbert's Theorem 90, there exists an element m in M^* such that

$$\frac{\sigma(m)}{m} = \varepsilon i.$$

Let $\delta = m^2\varepsilon$. We check that δ lies in $\mathbb{Q}(\sqrt{-1})$:

$$\sigma(\delta) = (\sigma(m))^2\sigma(\varepsilon) = m^2(\varepsilon i)^2\sigma(\varepsilon) = (m^2\varepsilon)(-\varepsilon\sigma(\varepsilon)).$$

Since $\varepsilon\sigma(\varepsilon) = -1$, σ does indeed fix δ. Clearly condition (1) is satisfied. For condition (2) we compute:

$$N_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\delta) = (m^2\varepsilon)\tau(m^2\varepsilon) = (\varepsilon m\tau(m))^2.$$

We need $(\varepsilon m\tau(m))^2 \equiv p_1 \dots p_k \bmod \mathbb{Q}^{*2}$. So it is enough to show that $\gamma = (\varepsilon m\tau(m))/\sqrt{p_1 \dots p_k}$ is in $\mathbb{Q}^*$. Since τ fixes ε and $\sqrt{p_1 \dots p_k}$, τ fixes γ. On the other hand, since $\varepsilon\sigma(\varepsilon) = -1$,

$$\sigma(\gamma) = \frac{-\varepsilon^{-1}\sigma(m)\tau(\sigma(m))}{-\sqrt{p_1 \dots p_k}} = \frac{\varepsilon^{-1}(m\varepsilon i)\tau(m\varepsilon i)}{\sqrt{p_1 \dots p_k}}.$$

Since τ fixes ε and maps i to $-i$, the above quotient reduces to γ. Thus γ is fixed by $\mathrm{Gal}(M/\mathbb{Q})$ and so lies in $\mathbb{Q}^*$. ■

By condition (1) in Lemma 4.5, we know that

$$(1+i,\varepsilon)_{\mathfrak{D}} = (1+i,\delta)_{\mathfrak{D}}.$$

Let D be the dyadic prime of $\mathbb{Q}(\sqrt{-1})$. Then D splits in M, with $\mathfrak{D}$ as one of the two primes of M lying over it. Thus

$$(1+i,\delta)_{\mathfrak{D}} = (1+i,\delta)_D.$$

As a result of Proposition 4.1 and Lemmas 4.2–4.5, we have shown:

(4.6) If condition (i) holds then $4\text{-rk}\, K_2\mathcal{O}_E = 0$ if and only if $(1+i,\delta)_D = -1$.

To complete the proof of our theorem, we show under the hypothesis $4\text{-rk}\, C(E) = 0$ and $N_{E/\mathbb{Q}}(\varepsilon) = -1$, that the condition $(1+i,\delta)_D = -1$ is equivalent to condition (ii) from the theorem.

Proof of Theorem 2.1. Since the p_j are congruent to 1 mod 4, they split in $\mathbb{Q}(\sqrt{-1})$. Let P_j and $\overline{P}_j$ be the primes of $\mathbb{Q}(\sqrt{-1})$ lying over p_j. From condition (2) in Lemma 4.5,

$$\mathrm{ord}_{P_j}(\delta) + \mathrm{ord}_{\overline{P}_j}(\delta) \equiv 1 \bmod 2.$$

So we may assume that $\mathrm{ord}_{P_j}(\delta) \equiv 1 \bmod 2$. By reciprocity,

$$\prod_Q (1+i,\delta)_Q = 1$$

where the product ranges over all primes Q of $\mathbb{Q}(\sqrt{-1})$. Let Q be a prime lying over $q \neq 2, p_1, \dots, p_k$ and let $\mathfrak{Q}$ be a prime of M lying over Q. Since $\mathfrak{Q}$ is unramified over Q, we have $\mathrm{ord}_{\mathfrak{Q}}(\delta) = \mathrm{ord}_Q(\delta)$. Using condition (1) from Lemma 4.5, we obtain

$$\mathrm{ord}_Q(\delta) \equiv 0 \bmod 2.$$

Thus, the only nontrivial factors in the product above occur at the primes lying over $2, p_1, \ldots, p_k$. Moreover, since $\mathrm{ord}_{\overline{P}_j}(\delta) \equiv 0 \bmod 2$, we have

$$(1+i,\delta)_D = \prod_{j=1}^{k}(1+i,\delta)_{P_j}.$$

Since $\mathrm{ord}_{P_j}(\delta) \equiv 1 \bmod 2$, $(1+i,\delta)_{P_j} = 1$ if and only if $1+i$ is a square mod P_j. Because $(1+i)^4 = -4$, we have

$$(1+i,\delta)_{P_j} = \left[\frac{-4}{P_j}\right]_8$$

where $\left[\frac{-4}{P_j}\right]_8$ is the 8th power symbol of -4 at P_j. We have shown that

$$(1+i,\delta)_D = \prod_{j=1}^{k}\left[\frac{-4}{P_j}\right]_8.$$

Since the inertial degree of P_j over p_j is 1, $\left[\frac{-4}{P_j}\right]_8 = 1$ exactly when -4 is an eighth power mod p_j. From [BC], this happens exactly when p_j can be represented over $\mathbb{Z}$ by the quadratic form x^2+32y^2. Thus, under the assumption $4\text{-rk}\, K_2\mathcal{O}_E = 0$, we have shown that $(1+i,\delta)_D = -1$ exactly when condition (ii) in the theorem holds. In light of (4.6), this completes the proof. ∎

5. Examples. We examine two quadratic fields for which $k=6$. In view of Remark 3.4, to apply the theorem we only need to check the graph Γ_E for nontrivial EVD's and count how many primes can be represented over $\mathbb{Z}$ by x^2+32y^2.

1) Let $E = \mathbb{Q}(\sqrt{17\cdot 73\cdot 89\cdot 97\cdot 137\cdot 233})$. Then Γ_E looks as in Figure 5.1. One can check that this graph has no nontrivial EVD's and that 137 is the only one of the primes that can be represented over $\mathbb{Z}$ by x^2+32y^2. Hence $4\text{-rk}\, K_2\mathcal{O}_E = 0$.

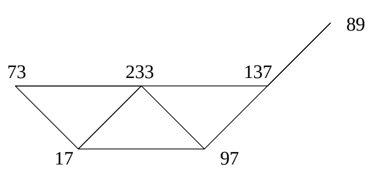

Fig. 5.1

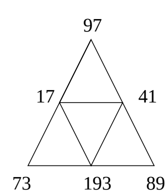

Fig. 5.2

2) Let $E = \mathbb{Q}(\sqrt{17\cdot 41\cdot 73\cdot 89\cdot 97\cdot 193})$. Then Γ_E looks as in Figure 5.2. Now 41 is the only one of the primes that can be represented over $\mathbb{Z}$ by

x^2+32y^2, but $\{\{17,41,193\},\{73,89,97\}\}$ is a nontrivial EVD. Thus $K_2\mathcal{O}_E$ has elements of order four.

References

[BC] P. Barrucand and H. Cohn, *Note on primes of type x^2+32y^2, class number and residuacity*, J. Reine Angew. Math. 238 (1969), 67–70.

[CH1] P. E. Conner and J. Hurrelbrink, *Class Number Parity*, Ser. Pure Math. 8, World Sci., Singapore, 1988.

[CH2] —, —, *Examples of quadratic number fields with $K_2\mathcal{O}$ containing no element of order four*, circulated notes, 1989.

[CH3] —, —, *The 4-rank of $K_2\mathcal{O}$*, Canad. J. Math. 41 (1989), 932–960.

[CH4] —, —, *On elementary abelian 2-Sylow K_2 of rings of integers of certain quadratic number fields*, Acta Arith. 73 (1995), 59–65.

[H] J. Hurrelbrink, *Circulant graphs and 4-ranks of ideal class groups*, Canad. J. Math. 46 (1994), 169–183.

Department of Mathematics
University of Michigan
Ann Arbor, Michigan 48109
U.S.A.
E-mail: vazzana@math.lsa.umich.edu

Received on 8.6.1996 (3003)