Chin. Ann. Math.
26B:2(2005),239–252.

ON IDEAL CLASS GROUPS AND UNITS IN TERMS OF THE QUADRATIC FORM $x^2 + 32y^2$[***]

Jurgen HURRELBRINK[*] YUE Qin[**]

Abstract

For quadratic number fields $F = \mathbb{Q}(\sqrt{2p_1 \cdots p_{t-1}}\,)$ with primes $p_j \equiv 1 \bmod 8$, the authors study the class number and the norm of the fundamental unit of F. The results generalize nicely what has been familiar for the fields $\mathbb{Q}(\sqrt{2p}\,)$ with a prime $p \equiv 1 \bmod 8$, including density statements. And the results are stated in terms of the quadratic form $x^2 + 32y^2$ and illustrated in terms of graphs.

Keywords Class group, Rédei Matrix, Fundamental unit
2000 MR Subject Classification 11R70, 11R11, 11R27

§ 1 . Introduction

It is a classical topic to study, for quadratic number fields $F = \mathbb{Q}(\sqrt{2p}\,)$ with a prime p, the exact 2-power dividing the narrow class number $h_+(F)$ and the norm of the fundamental unit ε of F.

The 2-primary subgroup of the narrow class group $C_+(F)$ is cyclic, and it is cyclic of order divisible by 4 if and only if $p \equiv 1 \bmod 8$. Well-known results on $h_+(F)$ and the norm of ε in the most interesting case are listed below in Corollary 3.3 in terms of the quadratic form $x^2 + 32y^2$. Equivalent statements can be found in various papers in the literature [3, 6, 7, 10–13, 18–20].

In this note, we are making an effort of generalizing results by replacing the fields $\mathbb{Q}(\sqrt{2p}\,)$ with quadratic fields

$$F = \mathbb{Q}(\sqrt{2p_1 \cdots p_{t-1}}\,) \quad \text{with primes} \quad p_j \equiv 1 \bmod 8, \quad j = 1, \cdots, t-1.$$

In Section 2 we handle the simple case of the 2-primary subgroup of $C_+(F)$ being elementary abelian. The main Section 3 is about the case of $C_+(F)$ being of 4-rank 1. So, the special case of $t = 2$ amounts to the classical one described above. The generalized results on the class number and the norm of the fundamental unit ε of F are stated in Theorem 3.1, Corollary 3.1, and Corollary 3.2. In Section 4 we present in Theorem 4.1 and Theorem 4.2

Manuscript received October 23, 2003. Revised April 1, 2004.

[*] Department of Mathematics, Louisiana State University, Baton Rouge, LA 70803-4918, USA.
E-mail: jurgen@math.lsu.edu

[**] Department of Mathematics, Nanjing University of Aeronautics and Astronautics, Nanjing 210016, China. **E-mail:** yueqin2@263.net

[***] Project supported by the National Natural Science Foundation of China (No.10371054) and 02KJB11 006.

an asymptotic formula and a density result concerning $N\varepsilon = -1$ for the fields F as above with 4-rank $C_+(F) = 1$, 8-rank $C_+(F) = 0$. Finally, in Section 5, Theorem 5.1, a result is obtained on the norm of the fundamental unit ε, generalizing the result (3.4), without any assumption on the 4-rank of $C_+(F)$.

Important in this paper are characterizations of primes in terms of quadratic forms, genus theory, Diophantine equations. Illustrations are being made in terms of graphs instead of Rédei matrices.

We use the following notations:

O_F	ring of integers of a number field F,
$C(F), C_+(F)$	ideal class group, narrow ideal class group of F,
$h(F), h_+(F)$	class number, narrow class number of F,
$[I]$	class of an ideal $I \subseteq O_F$ in $C_+(F)$,
ε	fundamental unit > 1 in a real quadratic field F,
${}_2A$	subgroup of elements of order ≤ 2 of an abelian group A,
$r_{2^n}(A)$	2^n-rank of A,
M_F	Rédei matrix of F,
Γ_F	graph associated with certain quadratic fields F,
A^+	set of primes $p \equiv 1 \bmod 8$ represented by $x^2 + 32y^2$ over $\mathbb{Z}$,
A^-	set of primes $p \equiv 1 \bmod 8$ not represented by $x^2 + 32y^2$ over $\mathbb{Z}$,
$2^n \parallel x$	2^n is the exact 2-power dividing x in $\mathbb{Z}$.

§ 2 . Rank $M_F = t - 1$

We consider real quadratic fields $F = \mathbb{Q}(\sqrt{d})$ with $d = 2p_1 \cdots p_{t-1}$ and distinct primes $p_j \equiv 1 \bmod 4$. Then -1 is a norm from the field F over $\mathbb{Q}$, and one is interested in the norm of the fundamental unit ε of F.

The Rédei matrix M_F of F is given as follows. Let $p_t = 2$ and denote by $\left(\frac{\cdot}{p}\right)$ the Legendre symbol if $p \neq 2$ and by $\left(\frac{\cdot}{2}\right)$ the Kronecker symbol. Then $M_F = (a_{ij})$ is the $t \times t$ matrix with $a_{ij} \in \mathbb{F}_2$ given by

$$(-1)^{a_{ij}} = \begin{cases} \left(\dfrac{p_j}{p_i}\right), & \text{if } i \neq j, \\ \left(\dfrac{d/p_i}{p_i}\right), & \text{if } i = j, \end{cases} \qquad i, j = 1, \cdots, t.$$

By Gauss, the 2-rank of the narrow ideal class group $C_+(F)$ is $t - 1$, and by Rédei's criterion (see [15–17]), the 4-rank of $C_+(F)$ is given by

$$r_4(C_+(F)) = t - 1 - \operatorname{rank} M_F. \tag{2.1}$$

In particular, $\operatorname{rank} M_F \leq t - 1$.

If M_F is of maximal rank $t - 1$, then the norm of the fundamental unit of F is known:

Proposition 2.1. *Let $F = \mathbb{Q}(\sqrt{d})$ with $d = 2p_1 \cdots p_{t-1}$, $p_j \equiv 1 \bmod 4$ for $j = 1, \cdots, t-1$ and let ε be the fundamental unit of F. If* $\operatorname{rank} M_F = t - 1$, *then* $N\varepsilon = -1$.

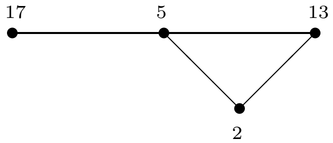
Proof. We have $r_2(C_+(F)) = t - 1$ and $r_4(C_+(F)) = 0$ by (2.1). Thus the 2-primary subgroup of $C_+(F)$ is elementary abelian of rank $t - 1$. Hence the exact 2-power dividing the narrow class number $h_+(F)$ of F is 2^{t-1}.

Since -1 is a field norm from F, the 2-rank of the ordinary class group $C(F)$ is also $t-1$ (compare 18.3 in [2]). Hence 2^{t-1} divides the ordinary class number $h(F)$ of F. Since $h_+(F)=h(F)$ or $2h(F)$, we conclude that $h_+(F)=h(F)$ and, in particular, $N\varepsilon=-1$.

When is the above maximal rank assumption satisfied? We have in Proposition 2.1: $\operatorname{rank} M_F=t-1$ if and only if the 2-primary subgroup of $C(F)$ is elementary abelian and $N\varepsilon=-1$.

As in [9], we associate with the field $F=\mathbb{Q}(\sqrt{2p_1\cdots p_{t-1}})$ the graph Γ_F on t vertices, labelled $p_1,\cdots,p_{t-1}$, $p_t=2$, with two distinct vertices p_i and p_j being adjacent if and only if $\left(\frac{p_i}{p_j}\right)=-1$. Here, for $p_i\equiv 1 \bmod 4$ and $p_t=2$, it is understood that $\left(\frac{p_i}{2}\right)=\left(\frac{2}{p_i}\right)=1$ if and only if $p_i\equiv 1 \bmod 8$.

For example, the graph Γ_F associated with the field $F=\mathbb{Q}(\sqrt{2\cdot 5\cdot 13\cdot 17})$ is given by



Combinatorial properties of Γ_F provide us with information about the 4-rank of $C_+(F)$. Namely, please compare [9]:

For a quadratic number field F as above with associated graph Γ_F, the 4-rank of the narrow class group $C_+(F)$ is given by

$$2^{r_4(C_+(F))}=\#\text{ of Eulerian vertex decompostions of }\Gamma_F. \tag{2.2}$$

Addendum 2.1. *If* $\operatorname{rank} M_F=t-1\geq 1$ *in Proposition* 2.1*, then* $d=2p_1\cdots p_{t-1}$ *has a prime divisor* $p_j\equiv 5 \bmod 8$.

Proof. If $t\geq 2$ and $p_j\equiv 1 \bmod 8$ for all $j=1,\cdots,t-1$, then $\left(\frac{2}{p_j}\right)=1$ for all j and Γ_F has an isolated vertex which implies by (2.2) that $r_4(C_+(F))\geq 1$ and hence, by (2.1), the rank of M_F is not $t-1$.

Illustration 2.1. In the basic case of $t=2$, $F=\mathbb{Q}(\sqrt{2p})$ with a prime $p\equiv 1 \bmod 4$, we note in terms of (2.2): If $p\equiv 5 \bmod 8$, then Γ_F is the graph ●—● which has only the trivial Eulerian vertex decomposition. Thus $r_4(C_+(F))=0$ and the 2-primary subgroup of $C_+(F)$ is cyclic of order 2. In particular, $\operatorname{rank} M_F=t-1=1$ and in fact, $M_F=\begin{pmatrix}1&1\\1&1\end{pmatrix}, h_+(F)=h(F)\equiv 2 \bmod 4$ and $N\varepsilon=-1$ (compare e.g. 19.8, 19.9 in [2]).

If $p\equiv 1 \bmod 8$, then Γ_F is the graph ● ● which has two Eulerian vertex decompositions. Thus $r_4(C_+(F))=1$ and the 2-primary subgroup of $C_+(F)$ is cyclic of order divisible by 4. In particular, $\operatorname{rank} M_F=t-2=0$. In fact, $M_F=\begin{pmatrix}0&0\\0&0\end{pmatrix}$, $h_+(F)\equiv 0 \bmod 4$ and the sign of the fundamental unit ε can be $+1$ as well as -1. Example: $N\varepsilon=+1$ with $\varepsilon=35+6\sqrt{34}$ in the case of $F=\mathbb{Q}(\sqrt{2\cdot 17})$ and $N\varepsilon=-1$ with $\varepsilon=9+\sqrt{82}$ in the case of $F=\mathbb{Q}(\sqrt{2\cdot 41})$ (compare e.g. 24.5 in [2]).

§ 3. Rank $M_F = t - 2$

We now consider the fields $F = \mathbb{Q}(\sqrt{2p_1 \cdots p_{t-1}})$ with $t \geq 2$ and all primes p_j being congruent to 1 mod 8. Then rank $M_F \leq t-2$ by Addendum 2.1 and our main emphasis is on the fields F with rank $M_F = t-2$; that is $r_4(C_+(F)) = 1$. Which fields F satisfy $N\varepsilon = -1$?

Definition 3.1. *The subsets A^+ and A^- of the set of all primes $p \equiv 1 \bmod 8$ are given by*

$A^+ = \{p \equiv 1 \bmod 8\colon\ p = x^2 + 32y^2 \text{ for some } x, y \in \mathbb{Z}\}$,

$A^- = \{p \equiv 1 \bmod 8\colon\ p \neq x^2 + 32y^2 \text{ for all } x, y \in \mathbb{Z}\}$.

In 21.6 in [2] it was shown that the sets A^+ and A^- both have density 1/8 as subsets of the set of all primes, and thus A^+ and A^- are of density 1/2 each in the set of primes $p \equiv 1$ mod 8.

For $F = \mathbb{Q}(\sqrt{2p_1 \cdots p_{t-1}})$, let the prime ideals $P_1, \cdots, P_{t-1}$ and $P_t = \mathcal{D}$ of O_F be given by $P_j^2 = p_j O_F$, in particular, $P_t^2 = \mathcal{D}^2 = 2O_F$ with $\mathcal{D}$ denoting the dyadic prime ideal of F. We prove via genus theory.

Theorem 3.1. *Let $F = \mathbb{Q}(\sqrt{d})$ with $d = 2p_1 \cdots p_{t-1}$, $p_j \equiv 1 \bmod 8$ for $j = 1, \cdots, t-1$ and suppose that* rank $M_F = t-2$. *Then*

(i) $[\mathcal{D}] \notin C_+(F)^4$ *if and only if* $p_1 \cdots p_{t-1} \equiv 9 \bmod 16$.

(ii) $[P_1 \cdots P_{t-1}] \notin C_+(F)^4$ *if and only if either* $p_1 \cdots p_{t-1} \equiv 9 \bmod 16$ *and an even number of the primes $p_1, \cdots, p_{t-1}$ belong to A^- or* $p_1 \cdots p_{t-1} \equiv 1 \bmod 16$ *and an odd number of the primes $p_1, \cdots, p_{t-1}$ belong to A^-.*

(iii) $[P_1 \cdots P_{t-1}\mathcal{D}] \notin C_+(F)^4$ *if and only if an odd number of the primes $p_1, \cdots, p_{t-1}$ belong to A^-.*

(iv) $[\mathcal{D}]$, $[P_1 \cdots P_{t-1}]$ *and* $[P_1 \cdots P_{t-1}\mathcal{D}]$ *lie in* $C_+(F)^4$ *if and only if* $p_1 \cdots p_{t-1} \equiv 1 \bmod 16$ *and an even number of the primes $p_1, \cdots, p_{t-1}$ belong to A^-.*

Proof. Since rank $M_F = t-2$, we have by (2.1) that $r_4(C_+(F)) = 1$. Hence the homogeneous system $M_F X = 0$ of t linear equations in t unknowns over $\mathbb{F}_2$ has only three nontrivial solutions $X = (0, \cdots, 0, 1)^T$, $(1, \cdots, 1, 0)^T$, $(1, \cdots, 1, 1)^T$, by e.g. [22]. Hence there are only the three ambiguous classes $[\mathcal{D}]$, $[P_1 \cdots P_{t-1}]$, $[P_1 \cdots P_{t-1}\mathcal{D}]$ in ${}_2C_+(F) \cap C_+(F)^2$. We are dealing with classes of order at most 2 that are squares in $C_+(F)$ with exactly one of the three classes being trivial, because of $r_4(C_+(F)) = 1$.

(i) In terms of norms from $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$, we have $p_1 \cdots p_{t-1} = u^2 - 2w^2 = 2(u+w)^2 - (u+2w)^2$ with $u, w \in \mathbb{N}$. Clearly, w is even and, without loss, $w \equiv 0 \bmod 4$ by multiplying $u + w\sqrt{2}$ by the element $(1+\sqrt{2})^2 = 3 + 2\sqrt{2}$ of norm $+1$, if necessary. We have $2p_1 \cdots p_{t-1} = 4(u+w)^2 - 2(u+2w)^2$ and thus

$$2(u+2w)^2 = (2(u+w))^2 - d \cdot 1^2. \tag{3.1}$$

Consequently, we obtain $[\mathcal{D}] = [P_{u+2w}]^2 \in C_+(F)^2$ for some ideal P_{u+2w} of O_F dividing $(u+2w)O_F$. By genus theory and [21] we conclude

$[\mathcal{D}] \in C_+(F)^4$

$\Longleftrightarrow [P_{u+2w}][P_m] \in C_+(F)^2$ where P_m denotes the ambiguous ideal over some divisor m of $p_1 \cdots p_{t-1}$.
$\Longleftrightarrow \left(\frac{d'(u+2w)}{p}\right) = \left(\frac{m(u+2w)}{l}\right) = 1$ for every odd prime $p|m$ and every odd prime $l|d'$ with $d' = d/m$.
$\Longleftrightarrow$ The linear system $M'_F X = (a_1, \cdots, a_{t-1})^T$ is solvable over $\mathbb{F}_2$ where M'_F is the $(t-1)\times t$ matrix obtained from the Rédei matrix M_F by deleting row t and the elements $a_j \in \mathbb{F}_2$ are given by $(-1)^{a_j} = \left(\frac{u+2w}{p_j}\right)$ for $j = 1, \cdots, t-1$.
$\Longleftrightarrow$ The Jacobi symbol $\left(\frac{u+2w}{p_1\cdots p_{t-1}}\right)$ is $+1$, by rank$M_F = t-2$.
$\Longleftrightarrow$ The Jacobi symbol $\left(\frac{2}{u+2w}\right)$ is $+1$, by (3.3) and quadratic reciprocity.
$\Longleftrightarrow u \equiv \pm 1 \bmod 8$.
$\Longleftrightarrow p_1 \cdots p_{t-1} \equiv 1 \bmod 16$.

(ii) In terms of norms from $\mathbb{Q}(\sqrt{-2})$ over $\mathbb{Q}$ we have in view of $p_j \equiv 1 \bmod 8$, $j = 1, \cdots, t-1$ that $p_j = a_j^2 + 2b_j^2$ with $a_j, b_j \in \mathbb{N}$, $b_j \equiv 0 \bmod 2$ and hence, for some $a, b \in \mathbb{N}$, a odd, b even,

$$p_1 \cdots p_{t-1} = a^2 + 2b^2.$$

Consequently, with a, b as above,

$$p_1 \cdots p_{t-1} a^2 = (p_1 \cdots p_{t-1})^2 - 2p_1 \cdots p_{t-1} b^2 \tag{3.2}$$

and $[P_1 \cdots P_{t-1}] = [P_a]^2 \in C_+(F)^2$ for some ideal P_a of O_F dividing aO_F. By Definition 3.1, we have $p_j \in A^+$ if and only if $b_j \equiv 0 \bmod 4$. By multiplicity of the norm, a straightforward induction yields that an even number of the primes $p_1, \cdots, p_{t-1}$ belong to A^- if and only if $b \equiv 0 \bmod 4$. In beautiful analogy with the proof in part (i) we now conclude

$[P_1 \cdots P_{t-1}] \notin C_+(F)^4$
$\Longleftrightarrow a \equiv \pm 3 \bmod 8$ in (3.4)
$\Longleftrightarrow$ either $p_1 \cdots p_{t-1} \equiv 9 \bmod 16$ and $b \equiv 0 \bmod 4$, or $p_1 \cdots p_{t-1} \equiv 1 \bmod 16$ and $b \equiv 2 \bmod 4$
$\Longleftrightarrow$ either $p_1 \cdots p_{t-1} \equiv 9 \bmod 16$ and an even number of the primes $p_1, \cdots, p_{t-1}$ belong to A^-, or $p_1 \cdots p_{t-1} \equiv 1 \bmod 16$ and an odd number of the primes $p_1, \cdots, p_{t-1}$ belong to A^-.

(iii) Let $\mathcal{D}$, P, $\mathcal{D}P$ stand for $[\mathcal{D}]$, $[P_1 \cdots P_{t-1}]$, $[\mathcal{D}P_1 \cdots P_{t-1}]$, respectively, being a 4-th power in $C_+(F)$. We summarize what we have proved in (i) and (ii) in terms of $p_1 \cdots p_{t-1}$ being 1 mod 16 or 9 mod 16 and in terms of an even or odd number of the primes $p_1, \cdots, p_{t-1}$ belonging to A^-, as follows:

	1(16)	9(16)
even	D P	not D not P
odd	D not P	not D P

.

In view of $[\mathcal{D}P_1 \cdots P_{t-1}] = [\mathcal{D}][P_1 \cdots P_{t-1}]$ and exactly one of the three classes being trivial in $C_+(F)$, the above table amounts to:

	1(16)	9(16)
even	D P DP	not D not P DP
odd	D not P not DP	not D P not DP

. (3.3)

In particular, $[\mathcal{D}P_1 \cdots P_{t-1}] \notin C_+(F)^4$ if and only if an odd number of the primes $p_1, \cdots, p_{t-1}$ belong to A^-, which proves claim (iii).

(iv) We just see from the table (3.3) that all three of $[\mathcal{D}]$, $[P_1 \cdots P_{t-1}]$, $[\mathcal{D}P_1 \cdots P_{t-1}]$ are in $C_+(F)^4$ if and only if $p_1 \cdots p_{t-1} \equiv 1 \bmod 16$ and an even number of the primes $p_1, \cdots, p_{t-1}$ belong to A^-, which proves claim (iv).

For the fields $F = \mathbb{Q}(\sqrt{2p_1 \cdots p_{t-1}})$ with $p_j \equiv 1 \bmod 8$, $j = 1, \cdots, t-1$, all three of -1, 2, -2 are norms from F over $\mathbb{Q}$. Concerning -1, 2, or -2 being a norm from O_F, we obtain:

Corollary 3.1. *Under the assumptions of Theorem* 3.1*, exactly one of* $-1, 2, -2$ *is a norm from* O_F*. Explicitly,* $-1, 2, -2$ *is a norm from* O_F *if and only if* $[\mathcal{D}P_1 \cdots P_{t-1}]$, $[\mathcal{D}]$, $[P_1 \cdots P_{t-1}]$*, respectively, is trivial in* $C_+(F)$*.*

Proof. Under our assumption of $\operatorname{rank} M_F = t-2$, that is $r_4(C_+(F)) = 1$, the claim follows in analogy to the well-known case of $t = 2$, $F = \mathbb{Q}(\sqrt{2p})$. Namely $[\mathcal{D}P_1 \cdots P_{t-1}]$ is trivial in $C_+(F)$ if and only if the ideal $(\sqrt{2p_1 \cdots p_{t-1}})O_F$ has a totally positive generator if and only if -1 is a norm from O_F. $[\mathcal{D}]$ is trivial in $C_+(F)$ clearly if and only if $+2$ is a norm from O_F. $[P_1 \cdots P_{t-1}]$ is trivial in $C_+(F)$ if and only if $p_1 \cdots p_{t-1}$ is a norm from O_F if and only if -2 is a norm from O_F.

Illustration 3.1. (i) In the special case of $F = \mathbb{Q}(\sqrt{2p})$ with a prime $p \equiv 1 \bmod 8$, the three cases of exactly one of $-1, 2, -2$ being a norm from O_F can be represented already by the three smallest primes $p \equiv 1 \bmod 8$. Namely,

for $p = 41$ we have $[\mathcal{D}P_1]$ is trivial and $N(9 + \sqrt{82}) = -1$,

for $p = 17$ we have $[\mathcal{D}]$ is trivial and $N(6 + \sqrt{34}) = 2$,

for $p = 73$ we have $[P_1]$ is trivial and $N(12 + \sqrt{146}) = -2$.

(ii) In Theorem 3.1, let $F = \mathbb{Q}(\sqrt{2p_1p_2})$ with distinct primes $p_1 \equiv p_2 \equiv 1 \bmod 8$ and $(\frac{p_1}{p_2}) = -1$.

For $p_1 = 17, p_2 = 41$, $[\mathcal{D}] \notin C_+(F)^4$, $[\mathcal{D}P_1P_2] \notin C(F)^4$ and $[P_1P_2] \in C(F)^4$.

For $p_1 = 41, p_2 = 89$, $[P_1P_2] \notin C_+(F)^4$, $[\mathcal{D}P_1P_2] \notin C(F)^4$ and $[\mathcal{D}] \in C_+(F)^4$.

For $p_1 = 17, p_2 = 73$, $[\mathcal{D}] \notin C_+(F)^4$, $[P_1P_2] \notin C_+(F)^4$ and $[\mathcal{D}P_1P_2] \in C(F)^4$.

For $p_1 = 17, p_2 = 97$, $[\mathcal{D}] \in C_+(F)^4$, $[P_1P_2] \in C_+(F)^4$ and $[\mathcal{D}P_1P_2] \in C(F)^4$.

In the general situation we conclude

Corollary 3.2. *Under the assumptions of Theorem* 3.1 *one has*

(i) $p_1 \cdots p_{t-1} \equiv 9 \bmod 16$ *and an even number of the primes* $p_1, \cdots, p_{t-1}$ *belong to* A^- *if and only if* $N\varepsilon = -1$ *and* $2^t \| h(F)$*.*

(ii) $p_1 \cdots p_{t-1} \equiv 1 \bmod 16$ *and an odd number of the primes* $p_1, \cdots, p_{t-1}$ *belong to* A^- *if and only if* 2 *is a norm from* O_F *and* $2^{t-1} \| h(F)$, *so* $N\varepsilon = +1$.

(iii) $p_1 \cdots p_{t-1} \equiv 9 \bmod 16$ *and an odd number of the primes* $p_1, \cdots, p_{t-1}$ *belong to* A^- *if and only if* -2 *is a norm from* O_F *and* $2^{t-1} \| h(F)$, *so* $N\varepsilon = +1$.

(iv) $p_1 \cdots p_{t-1} \equiv 1 \bmod 16$ *and an even number of the primes* $p_1, \cdots, p_{t-1}$ *belong to* A^- *if and only if* $r_8(C_+(F)) = 1$.

Proof. The claim follows directly from table (3.3) and Corollary 3.1 by having in mind that always $r_2(C_+(F)) = t-1$ and $r_4(C_+(F)) = 1$. For example, the case (iv) occurs if and only if all three classes $[\mathcal{D}P_1 \cdots P_{t-1}]$, $[\mathcal{D}]$, $[P_1 \cdots P_{t-1}]$ belong to $C_+(F)^4$.

In the special case of $t = 2$ we have reproved

Corollary 3.3. *Let* $F = \mathbb{Q}(\sqrt{2p})$ *with a prime* $p \equiv 1 \bmod 8$. *Then*

(i) $p \equiv 9 \bmod 16$ *and* $p \in A^+$ *if and only if* $N\varepsilon = -1$ *and* $4 \| h(F), 4 \| h_+(F)$.

(ii) $p \equiv 1 \bmod 16$ *and* $p \in A^-$ *if and only if* 2 *is a norm from* O_F *and* $2 \| h(F)$, $4 \|$ $h_+(F)$, *so* $N\varepsilon = +1$.

(iii) $p \equiv 9 \bmod 16$ *and* $p \in A^-$ *if and only if* -2 *is a norm from* O_F *and* $2 \| h(F), 4 \|$ $h_+(F)$, *so* $N\varepsilon = +1$.

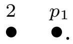
(iv) $p \equiv 1 \bmod 16$ *and* $p \in A^+$ *if and only if all three of* $[\mathcal{D}]$, $[\mathcal{D}P]$, $[P]$ *are in* $C_+(F)^4$ *if and only if* $8 | h_+(F)$.

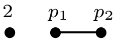
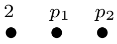
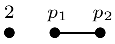
One might compare Corollary 3.3 to [1] and 24.4, 24.5 in [2]. In particular, we point out that Corollary 3.3 implies for $F = (\mathbb{Q}\sqrt{2p})$ with a prime $p \equiv 1 \bmod 8$ the well-known result:

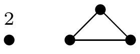
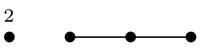
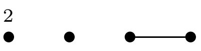
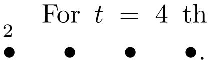
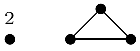
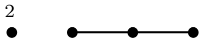
$$\text{if } \ p \in A^-, \quad \text{then } \ N\varepsilon = +1. \tag{3.4}$$

A generalization of the result (3.4) can be found below in Theorem 5.1.

Concerning Theorem 3.1 and its corollaries, it is in order to comment on when the assumption of $\operatorname{rank} M_F = t-2$ for $F = \mathbb{Q}(\sqrt{2p_1 \cdots p_{t-1}})$ with $p_j \equiv 1 \bmod 8$ for $j = 1, \cdots, t-1$ holds.

For $t = 2$ it is always satisfied, by Illustration 2.1. The graph Γ_F associated with F is .

For $t = 3$ the graph Γ_F is  or , representing the cases $r_4(C_+(F)) = 1$ or $r_4(C_+(F)) = 2$, respectively, by (2.2). So, the condition of $\operatorname{rank} M_F = t-2$ is satisfied if and only if Γ_F is . That amounts to $\left(\frac{p_1}{p_2}\right) = -1$, and is satisfied for example for $F = \mathbb{Q}(\sqrt{2 \cdot 17 \cdot 41})$.

For $t = 4$ the graph Γ_F is  or  or  or . We obtain from (2.2) that $r_4(C_+(F)) = 1$ holds exactly in the first two cases. So $\operatorname{rank} M_F = t-2$ if and only if Γ_F is given by  or  if and only if at least two of the three symbols $\left(\frac{p_1}{p_2}\right), \left(\frac{p_1}{p3}\right), \left(\frac{p_2}{p_3}\right)$ are -1. That is satisfied for examples for $F = \mathbb{Q}(\sqrt{2 \cdot 17 \cdot 41 \cdot 73})$ and $\mathbb{Q}(\sqrt{2 \cdot 17 \cdot 41 \cdot 97})$.

In fact, it follows from [15] that about 41.94% of all graphs Γ_F represent the case of $r_4(C_+(F)) = 1$, that is $\operatorname{rank} M_F = t-2$.

§ 4 . Density

Let $F = \mathbb{Q}(\sqrt{2p_1 \cdots p_{t-1}}\,)$ be a real quadratic field with distinct primes $p_j \equiv 1 \bmod 8$, $j = 1, \cdots, t-1$. Suppose that $\mathrm{rank} M_F = t-2$; that is, $r_4(C_+(F)) = 1$.

The first three cases of Theorem 3.1 amount to $r_8(C_+(F)) = 0$, by Corollary 3.2, which means $2^t \| h_+(F)$. Moreover, by Corollary 3.1, exactly one of $-1, 2, -2$ is a norm from O_F.

In this section we will discuss the following questions: How likely is it that $r_8(C_+(F)) = 0$ and $N\varepsilon = -1$? How likely is it that $r_8(C_+(F)) = 0$ and 2 is a norm from O_F? How likely is it that $r_8(C_+(F)) = 0$ and -2 is a norm from O_F?

Let x be a positive real number. We define

$$\begin{aligned}
A_t &= \{F = \mathbb{Q}(\sqrt{2p_1 \cdots p_{t-1}}\,) \text{ with distinct primes } p_j \equiv 1 \bmod 8\},\\
A_{t;x} &= \{F = \mathbb{Q}(\sqrt{2p_1 \cdots p_{t-1}}\,) \in A_t : \ p_1 \cdots p_{t-1} \le x\},\\
A_{t,t-2;x} &= \{F = \mathbb{Q}(\sqrt{2p_1 \cdots p_{t-1}}\,) \in A_{t;x} : \mathrm{rank} M_F = t-2 \text{ and } p_1 \cdots p_{t-1} \le x\},\\
A^{(-1)}_{t,t-2;x} &= \{F \in A_{t,t-2;x} : 2^t \| h_+(F) \text{ and } N\varepsilon = -1\},\\
A^{(2)}_{t,t-2;x} &= \{F \in A_{t,t-2;x} : 2^t \| h_+(F) \text{ and 2 is a norm from } O_F\},\\
A^{(-2)}_{t,t-2;x} &= \{F \in A_{t,t-2;x} : 2^t \| h_+(F) \text{ and } -2 \text{ is a norm from } O_F\}.
\end{aligned}$$

Fix $F' = \mathbb{Q}(\sqrt{2p'_1 \cdots p'_{t-1}}\,) \in A_{t;x}$, $p'_1 < p'_2 < \cdots < p_{p-1}$. Let $F = \mathbb{Q}(\sqrt{2p_1 \cdots p_{t-1}}\,) \in A_{t;x}$, $p_1 < p_2 < \cdots < p_{t-1}$. We will call F equivalent to F' if $\left(\frac{p_i}{p_j}\right) = \left(\frac{p'_i}{p'_j}\right) = (-1)^{u_{ij}}$, $u_{ij} \in \mathbb{F}_2$, for $1 \le i < j \le t-1$.

We put

$\delta(p_i, p_j) = 1$ if and only if $\left(\frac{p_i}{p_j}\right) = \left(\frac{p'_i}{p'_j}\right) = (-1)^{u_{ij}}$, $\delta(p_i, p_j) = 0$ otherwise, and $Y_j = \prod_{i=1}^{j-1} \delta(p_i, p_j)$ for $2 \le j \le t-1$.

We observe that the conditions $p_1 \cdots p_{t-1} \le x$ and $p_1 < \cdots < p_{t-1}$ imply

$$\begin{aligned}
&p_1 \le x^{1/(t-1)}, \quad p_1 < p_2 \le (x/p_1)^{1/(t-2)}, \cdots,\\
&p_{t-3} < p_{t-2} \le (x/p_1 \cdots p_{t-3})^{1/2}, \quad p_{t-2} < p_{t-1} \le x/p_1 \cdots p_{t-2}.
\end{aligned}$$

Lemma 4.1. *Fix* $F' \in A^{(i)}_{t,\,t-2;\,x}$, $i = -1,\ 2,\ -2$, *and let*

$$N(F') = \{F \in A^{(i)}_{t,t-2;x} \,|\, F \textit{ are equivalent to } F' \textit{ and } \quad p_1 \cdots p_{t-1} \le x\}.$$

Then, as $x \to \infty$,

$$|N(F')| \sim 2^{-(t^2+t)/2-1} \cdot \frac{1}{(t-2)!} \frac{x (\log\log x)^{t-2}}{\log x}. \tag{4.1}$$

Proof. In the following, we will use the same type of calculation as used in proving Lemma 3 in [4] to prove (4.1) (compare e.g. [23]).

Let $F' \in A^{(-1)}_{t,t-2;\,x}$. By Theorem 3.1, we now conclude

$$|N(F')| = \sum_{\substack{\text{an even number of } p_i\text{'s belong to } A^- \\ p_1\cdots p_{t-1}\equiv 9 \bmod 16}} \ \sum_{\substack{p_1\le x^{1/t-1} \\ p_1\equiv 1 \bmod 8}} \sum_{\substack{p_1<p_2\le (x/p_1)^{1/t-2} \\ p_2\equiv 1 \bmod 8}} Y_2 \cdots \sum_{\substack{p_{t-2}<p_{t-1}\le x/p_2\cdots p_{t-2} \\ p_{t-1}\equiv 1 \bmod 8}} Y_{t-1}. \tag{4.2}$$

We first consider

$$\sum_{\substack{p_{t-2}<p_{t-1}\le \frac{x}{p_1\cdots p_{t-2}} \\ p_{t-1}\equiv 1 \bmod 8}} Y_{t-1} = \sum_{\substack{p_{t-1}\le \frac{x}{p_1\cdots p_{t-2}} \\ p_{t-1}\equiv 1 \bmod 8}} Y_{t-1} - \sum_{\substack{p_{t-1}\le p_{t-2} \\ p_{t-1}\equiv 1 \bmod 8}} Y_{t-1}.$$

Since $p_{t-2} \le \left(\frac{x}{p_1\cdots p_{t-3}}\right)^{\frac{1}{2}}$,

$$\begin{aligned}\sum_{\substack{p_{t-1}\le p_{t-2} \\ p_{t-1}\equiv 1 \bmod 8}} Y_{t-1} &= O\Bigg(\sum_{p_{t-1}\le (\frac{x}{p_1\cdots p_{t-3}})^{\frac{1}{2}}} 1\Bigg) \\ &= O\left(\frac{\left(\frac{x}{p_1\cdots p_{t-3}}\right)^{\frac{1}{2}}}{\log\left(\frac{x}{p_1\cdots p_{t-3}}\right)^{\frac{1}{2}}}\right) = O\left(\frac{\left(\frac{x}{p_1\cdots p_{t-3}}\right)^{\frac{1}{2}}}{\log x}\right)\end{aligned}$$

for $p_1\cdots p_{t-3} \le x^{\frac{t-3}{t-1}}$. Then

$$O\Bigg(\sum_{p_{t-2}\le \left(\frac{x}{p_1\cdots p_{t-3}}\right)^{\frac{1}{2}}} \frac{\left(\frac{x}{p_1\cdots p_{t-3}}\right)^{\frac{1}{2}}}{\log x}\Bigg) = O\Big(\frac{x}{p_1\cdots p_{t-3}\log^2 x}\Big),$$

$$O\Bigg(\sum_{p_1\cdots p_{t-3}\le x^{\frac{t-3}{t-1}}} \frac{x}{p_1\cdots p_{t-3}\log^2 x}\Bigg) = O\Big(\frac{x(\log\log x)^{t-3}}{\log^2 x}\Big) = O\Big(\frac{x}{\log x}\Big).$$

Thus the terms with $\sum\limits_{p_{t-1}\le p_{t-2}} Y_{t-1}$ contribute only to the error term in Lemma 4.1.

To estimate $\sum\limits_{\substack{p_{t-1}\le \frac{x}{p_1\cdots p_{t-2}} \\ p_{t-1}\equiv 1 \bmod 8}} Y_{t-1}$, we have the relation

$$\begin{aligned}\sum_{\substack{p_{t-1}\le \frac{x}{p_1\cdots p_{t-2}} \\ p_{t-1}\equiv 1 \bmod 8}} Y_{t-1} &= \sum_{\substack{p_{t-1}\le \frac{x}{p_1\cdots p_{t-2}} \\ p_{t-1}\equiv 1 \bmod 8}} \prod_{j=1}^{t-2} \frac{1}{2}\Big(1+(-1)^{u_{t-1,j}}\Big(\frac{p_{t-1}}{p_j}\Big)\Big) \\ &= \frac{1}{2^{t-2}} \sum_{\substack{p_{t-1}\le \frac{x}{p_1\cdots p_{t-2}} \\ p_{t-1}\equiv 1 \bmod 8}} 1 + O\Bigg(\sum_{\chi\ne 1} \sum_{\substack{p_{t-1}\le \frac{x}{p_1\cdots p_{t-2}} \\ p_{t-1}\equiv 1 \bmod 8}} \chi_{p_1\cdots p_{t-2}}(p_{t-1})\Bigg) \\ &\sim \frac{1}{2^t}\frac{\frac{x}{p_1\cdots p_{t-2}}}{\log\frac{x}{p_1\cdots p_{t-2}}} + O\Bigg(\sum_{\chi\ne 1} \sum_{\substack{p_{t-1}\le \frac{x}{p_1\cdots p_{t-2}} \\ p_{t-1}\equiv 1 \bmod 8}} \chi_{p_1\cdots p_{t-2}}(p_{t-1})\Bigg),\end{aligned} \tag{4.3}$$

where each $\chi_{p_1\cdots p_{t-2}}$ is the product of some Legendre symbols $\left(\frac{\cdot}{p_j}\right), j=1,\cdots,t-2$. By [4, pp.202–203], we can know that

$$\sum_{\substack{p_1\le x^{\frac{1}{t-1}}\\ p_1\equiv 1 \bmod 8}} \cdots \sum_{\substack{p_{t-3}<p_{t-2}\le\left(\frac{x}{p_1\cdots p_{t-3}}\right)^{\frac12}\\ p_{t-2}\equiv 1 \bmod 8}} Y_{t-2} \sum_{\substack{p_{t-1}\le\frac{x}{p_1\cdots p_{t-2}}\\ p_{t-1}\equiv 1 \bmod 8}} \chi_{p_1\cdots p_{t-2}}(p_{t-1})$$
$$= o\Big(\frac{x(\log\log x)^{t-2}}{\log x}\Big). \tag{4.4}$$

Thus

$$|N(F')| = \sum_{\substack{\text{even number of } p_i\in A^-\\ p_1\cdots p_{t-1}\equiv 9 \bmod 16}} \sum_{\substack{p_1\le x^{\frac{1}{t-1}}\\ p_1\equiv 1 \bmod 8}} \sum_{\substack{p_1<p_2\le(\frac{x}{p_1})^{\frac{1}{t-2}}\\ p_2\equiv 1 \bmod 8}} Y_2$$
$$\cdots \sum_{\substack{p_{t-3}<p_{t-2}\le\left(\frac{x}{p_1\cdots p_{t-3}}\right)^{\frac12}\\ p_{t-2}\equiv 1 \bmod 8}} \frac{Y_{t-2}}{2^t}\frac{x}{p_1\cdots p_{t-2}\log x} + o\Big(\frac{x(\log\log x)^{t-2}}{\log x}\Big). \tag{4.5}$$

Next we can apply the same procedure to Y_{t-2} that we applied to Y_{t-1} (i.e., note the relation (4.3)). Then the main term in

$$\sum_{\substack{p_{t-3}<p_{t-2}\le(\frac{x}{p_1\cdots p_{t-3}})^{\frac12}\\ p_{t-2}\equiv 1 \bmod 8}} \frac{Y_{t-2}}{2^t}\cdot\frac{x}{p_1\cdots p_{t-2}\log x}$$

is

$$\sum_{p_{t-3}<p_{t-2}\le(\frac{x}{p_1\cdots p_{t-3}})^{\frac12}} \frac{1}{2^t2^{t-1}}\cdot\frac{x}{p_1\cdots p_{t-2}\log x}.$$

The same procedure can be applied to each Y_i, $2\le i\le t-1$. The main term in (4.2), a factor of $\frac14$ is introduced by the condition $p_1\equiv 1 \bmod 8$ and a factor of $\frac14$ is introduced by the condition of an even number of $p_1,\cdots,p_{t-1}$ belonging to A^- and $p_1\cdots p_{t-1}\equiv 9 \bmod 16$ (note that it is equally likely to be $p\in A^+$ or $p\in A^-$ for a prime $p\equiv 1 \bmod 8$ in [2, 21.6]). Hence we obtain the following main term in $|N(F')|$:

$$\sum_{p_1\le x^{\frac{1}{t-1}}} \sum_{p_1<p_2\le(\frac{x}{p_1})^{\frac{1}{t-2}}} \cdots \sum_{p_{t-3}<p_{t-2}\le(\frac{x}{p_1\cdots p_{t-3}})^{\frac12}} \frac{1}{2^{t+(t-1)+\cdots+1+1}}\cdot\frac{x}{p_1\cdots p_{t-2}\log x}$$
$$\sim \frac{1}{2^{\frac{t^2+t}{2}+1}}\frac{x}{\log x}\sum_{\substack{p_1\cdots p_{t-2}\le x^{\frac{t-2}{t-1}}\\ p_1<\cdots<p_{t-2}}}\frac{1}{p_1\cdots p_{t-2}} \sim 2^{-\frac{t^2+t}{2}-1}\cdot\frac{1}{(t-2)!}\cdot\frac{x(\log\log x)^{t-2}}{\log x}$$

by [8, Chapter XXII]. To finish the proof of Lemma 4.1, it remains to show that the other terms in Equation (4.5) are $o\left(\frac{x(\log\log x)^{t-2}}{\log x}\right)$. By [4, pp.204–206], we can know that

$$\sum_{p_1\le x^{\frac{1}{t-1}}} \sum_{p_1<p_2\le(\frac{x}{p_1})^{\frac{1}{t-2}}} Y_2\cdots \sum_{p_{t-3}<p_{t-2}\le(\frac{x}{p_1\cdots p_{t-3}})^{\frac12}} \frac{\chi_{p_1\cdots p_{t-3}}(p_{t-2})}{p_1\cdots p_{t-2}} = o((\log\log x)^{t-2}),$$

where $\chi_{p_1\cdots p_{t-3}}$ is the product of some Legendre symbols $\left(\frac{\cdot}{p_j}\right), j=1,\cdots,t-3$, analogous to Equation (4.4). Similar calculations can be carried out for the nontrivial characters that come from equations for $Y_{t-1},\cdots,Y_2$ analogous to Equation (4.4).

Our proof of Lemma 4.1 is completed.

Theorem 4.1. *For $t\geq 2$, as $x\to\infty$, we have for the orders of these sets asymptotically,*

$$|A^{(-1)}_{t,t-2;x}|\sim|A^{(2)}_{t,t-2;x}|\sim|A^{(-2)}_{t,t-2;x}|\sim\frac{S(t-2)}{2^{(t^2+t)/2+1}\cdot(t-2)!}\frac{x(\log\log x)^{t-2}}{\log x},$$

where $S(t-2)$ is the number of invertible symmetric $(t-2)\times(t-2)$ matrices over $\mathbb{F}_2$.

Addendum 4.1. *$S(t-2)$ is given by (compare e.g.* [14, *Lemma* 18])

$$S(t-2)=2^{\epsilon(t-2)}\prod_{k=0}^{[(t-3)/2]}(2^{2k+1}-1), \tag{4.6}$$

$$\epsilon(t-2)=\begin{cases}\dfrac{(t-2)^2-1}{4}, & \textit{if } t-2 \textit{ is odd},\\ \dfrac{(t-2)^2+2(t-2)}{4}, & \textit{if } t-2 \textit{ is even},\end{cases}$$

where $[x]$ denotes the greatest integer $\leq x$ and the product is 1 for $t=2$.

Proof. We identify fields in the given sets according to the above equivalence relation. For every field F in $A^{(-1)}_{t,t-2;x}$, the Rédei matrix M_F is a symmetric $t\times t$ matrix over $\mathbb{F}_2$ of $\operatorname{rank} M_F=t-2$. It follows that for x sufficiently large, the number of equivalence classes in $A^{(-1)}_{t,t-2;x}$ is the number of invertible symmetric $(t-2)\times(t-2)$ matrices over $\mathbb{F}_2$; it is explicitly given by $S(t-2)$ in (4.6).

Fix $F'=\mathbb{Q}(\sqrt{2p'_1\cdots p'_{t-1}})\in A^{(-1)}_{t,t-2;x}$. Let $N(F')$ denote the set of fields F in $A^{(-1)}_{t,t-2;x}$ that are equivalent to F'. By multiplying $|N(F')|$ in (4.1) by $S(t-2)$ from (4.6), we conclude that, as $x\to\infty$,

$$|A^{(-1)}_{t,t-2;x}|\sim\frac{S(t-2)}{2^{(t^2+t)/2+1}\cdot(t-2)!}\frac{x(\log\log x)^{t-2}}{\log x}.$$

Analogously, via Theorem 3.1, the same estimates are obtained also for $|A^{(2)}_{t,t-2;x}|$ and $|A^{(-2)}_{t,t-2;x}|$.

Now we investigate how likely it is that $\operatorname{rank} M_F=t-2$, $2^t\|h_+(F)$, and $N\varepsilon=-1$ for these fields F in A_t. Since for every field F in A_t the Rédei matrix M_F is symmetric, it follows that, for x sufficiently large, the number of equivalence classes of fields F in $A_{t;x}$ is $2^{(t-1)(t-2)/2}$, and it is left to count the number of possible Rédei matrices of fields F in a given equivalence class.

As before, fix a field $F'=\mathbb{Q}(\sqrt{2p'_1\cdots p'_{t-1}})\in A_{t;x}$, and let $M(F')$ denote the set of fields F in $A_{t;x}$ that are equivalent to F'. Then, as $x\to\infty$,

$$\begin{aligned}|M(F')|&=\sum_{\substack{p_1\leq x^{1/t-1}\\ p_1\equiv 1 \bmod 8}}\ \sum_{\substack{p_1\leq p_2\leq(x/p_1)^{1/t-2}\\ p_2\equiv 1 \bmod 8}} Y_2\cdots\sum_{\substack{p_{t-2}\leq p_{t-1}\leq x/p_2\cdots p_{t-2}\\ p_{t-1}\equiv 1 \bmod 8}} Y_{t-1}\\ &\sim 2^{-(t^2+t)/2+1}\cdot\frac{1}{(t-2)!}\frac{x(\log\log x)^{t-2}}{\log x}\end{aligned}$$

and thus

$$|A_{t;x}| \sim \frac{2^{(t-1)(t-2)/2}}{2^{(t^2+t)/2-1} \cdot (t-2)!} \frac{x(\log\log x)^{t-2}}{\log x}. \tag{4.7}$$

By combining Theorem 4.1 with (4.13), we have obtained

Theorem 4.2. *For $t \geq 2$ one has*

$$\lim_{x\to\infty} \frac{|A^{(i)}_{t,t-2;x}|}{|A_{t;x}|} = \frac{S(t-2)}{2^{(t-1)(t-2)/2+2}}, \qquad i = -1,\ 2,\ -2.$$

Let us consider the results in the classical case of $t = 2$. The universe is given by

$$A_2 = \{F = \mathbb{Q}(\sqrt{2p}\,) :\ p \text{ prime},\ p \equiv 1 \bmod 8\}.$$

Since the Rédei matrix of such fields is the zero matrix of size 2×2, we have $A_{t;x} = A_{t,t-2;x}$ for $t = 2$.

By Theorem 4.1, the three sets

$$\begin{aligned}
&\{F \in A_2 : r_8(C_+(F)) = 0 \text{ and } N\varepsilon = -1\},\\
&\{F \in A_2 : r_8(C_+(F)) = 0 \text{ and } 2 \text{ is a norm from } O_F\},\\
&\{F \in A_2 : r_8(C_+(F)) = 0 \text{ and} -2 \text{ is a norm from } O_F\}
\end{aligned}$$

are of density $\frac{1}{4}$ each in A_2.

All of that is clearly consistent with Corollary 3.3 and consequently also the set

$$\{F \in A_2 : r_8(C_+(F)) = 1\}$$

is of density $\frac{1}{4}$ in A_2, too. For earlier proofs of these density statements in this special case we can refer to [18] and ongoing work by LSU graduate student C. Ionita.

§ 5. Rank $M_F \leq t-2$

As before, we consider fields $F = \mathbb{Q}(\sqrt{2p_1 \cdots p_{t-1}}\,)$ with distinct primes $p_j \equiv 1 \bmod 8$, $j = 1, \cdots, t-1$. We will present in this section a result on the norm of the fundamental unit ε of F, that is a pretty generalization of the result (3.4) without any restriction on t or the rank of M_F.

The primes $p = x^2 + 32y^2$ in A^+ can be characterized also in the following way:

Lemma 5.1. *For primes $p \equiv 1 \bmod 8$, the following are equivalent:*

(i) $p \in A^+$.

(ii) $p = a^2 + b^2$ *for some* $a, b \in \mathbb{N}$ *with* $a + b \equiv \pm 1 \bmod 8$.

(iii) $2p = e^2 + f^2$ *for some* $e, f \in \mathbb{N}$ *with* $e, f \equiv \pm 1 \bmod 8$.

Proof. For the equivalence of (ii) and (iii) we note that $p = a^2 + b^2$ if and only if $2p = (a+b)^2 + (a-b)^2$. It is enough to prove the equivalence of (i) and (iii).

Start with condition (iii). Then $2p = e^2 + f^2$ with $e, f \in \mathbb{N}$, $e, f \equiv \pm 1 \bmod 8$; that is, $(2p)^2 - 2pf^2 = 2pe^2$ with $e, f \in \mathbb{N}$ as above. This is equivalent to the Diophantine equation

$ez^2 = x^2 - 2py^2$ being solvable with $x,\ y,\ z \in \mathbb{Z}$ by the way we proved Theorem 3.1, part (i). Equivalently, with $F = \mathbb{Q}(\sqrt{2p}\,)$ we have: $[P_e] \in C_+(F)^2$ for the class $[P_e]$ in $C_+(F)$ of some ideal P_e dividing eO_F. That is equivalent to the class of $\mathcal{D}P$, that is the class of the ideal $\sqrt{2p}O_F$, being a fourth power in $C_+(F)$. Finally, $[\mathcal{D}P] \in C_+(F)^4$ is equivalent, for example by the table (3.3), to $p \in A^+$, which is the condition (i).

Here is the generalization of the result (3.4).

Theorem 5.1. *Let $F = \mathbb{Q}(\sqrt{2p_1 \cdots p_{t-1}}\,)$ with distinct primes $p_j \equiv 1 \bmod 8$ for $j = 1, \cdots, t-1$. Let ε be the fundamental unit of F. Suppose that an odd number of the primes $p_1, \cdots, p_{t-1}$ belong to A^-. Then $N\varepsilon = +1$.*

Proof. We have $2p_1 \cdots p_{t-1} = e^2 + f^2$ for some $e,\ f \in \mathbb{N}$ and hence $(2p_1 \cdots p_{t-1})^2 - 2p_1 \cdots p_{t-1}f^2 = 2p_1 \cdots p_{t-1}e^2$; so, $[P_1 \cdots P_t\mathcal{D}] = [P_e]^2$ for some ideal P_e dividing eO_F. Let M' be the $(t-1) \times t$ matrix obtained from M_F by deleting row t. By the way, the t-th row is a zero row since $\left(\frac{p_j}{2}\right) = +1$ for $j = 1, \cdots, t-1$. Again we refer to how we proved Theorem 3.1 part (i) and obtain the equivalences: $[P_1 \cdots P_{t-1}\mathcal{D}] \in C_+(F)^4$ if and only if $[P_m][P_e] \in C_+(F)^2$ for some ideal P_m dividing mO_F for some $m | p_1 \cdots p_{t-1}$ if and only if the system $M'_F X = (e_1, \cdots, e_{t-1})^T$ is solvable over $\mathbb{F}_2$ where $(-1)^{e_i} = \left(\frac{e}{p_i}\right)$ for $i = 1, \cdots, t-1$.

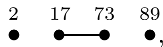
We now make use of the assumption that an odd number of the primes $p_1, \cdots, p_{t-1}$ belong to A^-. By Lemma 5.1 and an induction one obtains

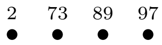
$$\begin{aligned} p_1 \cdots p_{t-1} &= a^2 + b^2 \qquad \text{with } a,\ b \in \mathbb{N},\ a + b \equiv \pm 3 \bmod 8, \\ 2p_1 \cdots p_{t-1} &= e^2 + f^2 \qquad \text{with } e,\ f \in \mathbb{N},\ e,\ f \equiv \pm 3 \bmod 8. \end{aligned}$$

Thus $\left(\frac{2p_1 \cdots p_{t-1}}{e}\right) = 1$ and $\left(\frac{e}{p_1 \cdots p_{t-1}}\right) = -1$ by quadratic reciprocity in view of $e \equiv \pm 3 \bmod 8$. We have obtained that $\left(\frac{e}{p_j}\right) = -1$ happens an odd number of times. Now the sum of the $t-1$ rows of M'_F is the zero row. Hence the system $M'_F X = (e_1, \cdots, e_{t-1})^T$ has no solution over $\mathbb{F}_2$.

Thus $[P_1 \cdots P_{t-1}\mathcal{D}] \notin C_+(F)^4$ by the equivalence derived at the beginning of the proof. So, the class $[P_1 \cdots P_{t-1}\mathcal{D}]$ is not trivial in $C_+(F)$ and hence there is no unit in O_F^* of norm -1; that is, $N\varepsilon = +1$.

We remark that Theorem 5.1 also generalizes what was obtained in Corollary 3.2 (ii) and (iii) under the assumption of rank $M_F = t - 2$. Now the result on $N\varepsilon = +1$ has been obtained also for fields $F = \mathbb{Q}(\sqrt{2p_1 \cdots p_{t-1}}\,)$ with rank $M_F < t - 2$. We illustrate Theorem 5.1 by giving numerical examples.

Example 5.1. Let $F = \mathbb{Q}(\sqrt{2 \cdot 17 \cdot 73 \cdot 89}\,)$. The graph Γ_F on $t = 4$ vertices is given by , so $r_4(C_+(F)) = 2$ by (2.2) and hence rank $M_F = t - 3$. Since all three primes $17, 73, 89$ belong to A^-, we obtain from Theorem 5.1 without any computation that $N\varepsilon = +1$.

Now let $F = \mathbb{Q}(\sqrt{2 \cdot 73 \cdot 89 \cdot 97}\,)$. Again we have $t = 4$. This time the graph Γ_F is the totally disconnected graph  since all symbols $\left(\frac{p_i}{p_j}\right)$ are $+1$. So $r_4(C_+(F)) = 3$ by (2.2), and rank $M_F = 0 = t - 4$. Also in this extreme case of the Rédei matrix being the zero matrix, Theorem 5.1 applies and we see just by inspection that $N\varepsilon = +1$.

References

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

[2] Conner, P. E. & Hurrelbrink, J., Class Number Parity, Ser. Pure Math. 8, World Scientific, Singapore, 1988.

[3] Conner, P. E. & Hurrelbrink, J., On the 4-rank of the tame kernel $K_2(\mathcal{O})$ in positive definite terms, *J. Number Th.*, **88**(2001), 263–282.

[4] Gerth III, F., Counting certain number fields with prescribed l-class numbers, *J. Reine Angew. Math.*, **337**(1982), 195–207.

[5] Gerth III, F., The 4-class ranks of quadratic fields, *Invent. Math.*, **77**(1984), 489–515.

[6] Hasse, H., Über die Klassenzahl Abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952; New edition, Springer-Verlag, 1985.

[7] Hasse, H., Über die Teilbarkeit durch 2^3 der Klassenzahl der quadratischen Zahlkörper mit genan zwei verschiedenen Diskriminantenprimteilern, *Math. Nachr.*, **46**(1970), 61–70,

[8] Hardy, G. & Wright, E., An Introduction to the Theory of Numbers (Fifth Edition), London, 1979.

[9] Hurrelbrink, J., Circulant graphs and 4-ranks of ideal class groups, *Can. J. Math.*, **46:**1(1994), 169–183

[10] Kaplan, P., Divisibilité par 8 du nombre des classes des corps quadratique dont le 2-groupe des classes est cyclique, et réciprocité biquadratique, *J. Math. Soc. Japan*, **25**(1973), 596–608.

[11] Kaplan, P. & Williams, K. S., On the class number of $\mathbb{Q}(\sqrt{\pm 2p})$ modulo 16 for $p \equiv 1 \pmod 8$ a prime, *Acta Arith.*, **40:**3(1982), 289–296.

[12] Kaplan, P. & Williams, K. S., On the strict class number of $\mathbb{Q}(\sqrt{2p})$ modulo 16, *Osaka J. Math.*, **21**(1984), 23–29.

[13] Lagarias, J. C., On determining the 4-rank of the ideal class group of a quadratic field, *J. Number Th.*, **12**(1980), 191–196.

[14] Morton, P., Density results for the 2-classgroups of imaginary quadratic fields, *J. Reine Angew. Math.*, **332**(1982), 156–187.

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

[16] Rédei, L., Arithmetischer Beweis des Satzes über die Anzahl der durch vier teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, *J. Reine Angew. Math.*, **171**(1934), 55–60.

[17] Rédei, L., Über einige Mittelwertfragen im quadratischen Zahlkörper, *J. Reine Angew. Math.*, **174**(1936), 131–148.

[18] Stevenhagen, P., Divisibility by 2-powers of certain quadratic class numbers, *J. Number Th.*, **43**(1993), 1–19.

[19] Yamamoto, Y., Divisibity by 16 of class numbers of quadratic fields whose 2-class groups are cyclic, *Osaka J. Math.*, **21**(1984), 1–22.

[20] Yamamoto, Y., Class number problems for quadratic fields (concentrating on the 2-part) (in Japanese), *Sûgaku*, **40**(1988), 167–174.

[21] Yue, Q., Dyadic ideal, class group, tame kernel in quadratic number fields, *J. Pure Appl. Algebra*, **166:**1-2(2002), 229–238.

[22] Yue, Q. & Feng, K., The 4-rank of the tame kernel versus the 4-rank of the narrow class group in quadratic number fields, *Acta Arith.*, **96:**2(2000), 155–165.

[23] Yue, Q. & Yu, J., The densities of 4-ranks of tame kernels for quadratic fields, *J. Reine Angew. Math.*, **567**(2004), 151–173