ON THE CLASS NUMBER OF A UNIT LATTICE OVER A RING OF REAL QUADRATIC INTEGERS

Mimura, Yoshio

ETD

http://hdl.handle.net/11094/27761

Osaka University
ON THE CLASS NUMBER OF A UNIT LATTICE OVER
A RING OF REAL QUADRATIC INTEGERS

YOSHIO MIMURA
§ 1. Introduction. Let $K$ be a totally real algebraic number field. In a positive definite quadratic space over $K$ a lattice $E_n$ is called a unit lattice of rank $n$ if $E_n$ has an orthonormal basis $\{e_1, \ldots, e_n\}$. The class number one problem is to find $n$ and $K$ for which the class number of $E_n$ is one. Dzewas ([1]), "Nebelung" ([3]), Pfeuffer ([6],[7]) and Peters ([5]) have settled this problem. The present state of this problem is: If $n \geq 3$, then the class number of $E_n$ is one if and only if "$K = \mathbb{Q}$, $n \leq 8$", "$K = \mathbb{Q}(\sqrt{2})$, $n \leq 4$", "$K = \mathbb{Q}(\sqrt{3})$, $n \leq 4$", "$K = \mathbb{Q}(\sqrt{7})$, $n = 3$", "$K = K(49)$, $n = 3$" or "$K = K(148)$, $n = 3$", where $\mathbb{Q}$ is the rational number field and $K(49)$ (resp. $K(148)$) is the unique totally real cubic number field with discriminant 49 (resp. 148). The class number two problem has been studied by Pohst ([10]), who gets a nearly complete result for $n \geq 4$: If $n \geq 4$, then the class number of $E_n$ is two only if "$K = K(49)$, $n = 4$" or "$K = \mathbb{Q}(\sqrt{3})$, $n = 5, 6, 7$", and the class number of $E_n$ is two in the first two cases. Pfeuffer ([8]) has shown that the class number of $E_n$ is three for $K = \mathbb{Q}(\sqrt{3})$ and $n = 6$. In the special case that $K$ is a real quadratic field, it remains to consider the class number of $E_3$ over $K (\neq \mathbb{Q}(\sqrt{2}), \mathbb{Q}(\sqrt{3}), \mathbb{Q}(\sqrt{7}))$.

All former proofs of the "only if" assertions and nearly all proofs of the class number one (or two) for special fields $K$ and special $n$ use the Siegel Mass Formula. On the other hand we have another method by which Kneser ([2]) has found the class number of $E_n$ for $\mathbb{Q}$. Using this method Salamon ([11]) has found the first result for $\mathbb{Q}(\sqrt{3})$. In this paper we shall prove the following theorem by using the Kneser method.
Theorem. In the case of real quadratic fields with $n \geq 3$, the class number of $E_n$ is two if and only if

$\mathbb{Q}(\sqrt{2})$, $n = 5$,

$\mathbb{Q}(\sqrt{3})$, $n = 3$,

$\mathbb{Q}(\sqrt{5})$, $n = 5$,

$\mathbb{Q}(\sqrt{13})$, $n = 3$,

$\mathbb{Q}(\sqrt{33})$, $n = 3$,

$\mathbb{Q}(\sqrt{41})$, $n = 3$.

The class number of $E_n$ is a monotone increasing function of $n$ for a fixed field $K$ ([4], 105:1). In §2 we discuss some properties of adjacent lattices. In §3 we find some special adjacent lattices to $E_n$ and prove that the class number of $E_n$ is more than two unless $K$ is one of the exceptional eight fields (Cf. Proposition 8). In §4 we treat the above exceptional cases and determine the class number by using Kneser method. The notation used in this paper will generally be those of [4].

§ 2. Adjacent lattices. Let $p$ be an odd prime number. Put

$$A^n_p = \{(a_1, \ldots, a_n) \in \mathbb{Z}^n; \sum_{i=1}^n a_i^2 \equiv 0 \mod p, (a_1, \ldots, a_n) \neq (0, \ldots, 0) \mod p\}$$

where $\mathbb{Z}$ is the ring of rational integers. We define an equivalence relation $\sim$ on $A^n_p : (a_1, \ldots, a_n) \sim (b_1, \ldots, b_n)$ if and only if there is a permutation $\{1', 2', \ldots, n'\}$ of $\{1, 2, \ldots, n\}$ and an integer $c$ prime to $p$ such that $b_i^2 \equiv c a_i^2 \mod p$ for all $i$. In each equivalence class we can choose a representative $(a_1, \ldots, a_n)$ satisfying

$$0 \leq a_1 \leq a_2 \leq \cdots \leq a_n$$

and

$$\sum_{i=1}^n a_i^2 = \sum_{i=1}^n b_i^2$$

for all $(b_1, \ldots, b_n)$ in the class.
By $\mathbb{R}_p^n$ we denote the set of the above representatives. Let $(a_1, \ldots, a_n)$ and $(b_1, \ldots, b_n)$ be in the same class and $(a_1, \ldots, a_n) \in \mathbb{R}_p^n$. We define the norm and the type of $(b_1, \ldots, b_n)$ (or the class):

\[ N(b_1, \ldots, b_n) = \frac{1}{p} \sum_{i=1}^{n} a_i^2, \]

\[ T(b_1, \ldots, b_n) = \min \{ \sum_{i=1}^{n} c_i^2 : \sum_{i=1}^{n} c_i b_i \equiv 0 \mod p, (c_1, \ldots, c_n) \neq (0, \ldots, 0) \}. \]

It is easy to prove the following proposition.

**Proposition 1.** The number of the equivalence classes of the specified type $T$ in $\mathbb{A}_p^3$ is as follows:

<table>
<thead>
<tr>
<th></th>
<th>$T = 1$</th>
<th>$T = 2$</th>
<th>$T = 3$</th>
<th>$T \geq 4$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$p = 3$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>$p \equiv 1 \mod 24$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>$(p-25)/24$</td>
</tr>
<tr>
<td>$p \equiv 5 \mod 24$</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>$(p-5)/24$</td>
</tr>
<tr>
<td>$p \equiv 7 \mod 24$</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>$(p-7)/24$</td>
</tr>
<tr>
<td>$p \equiv 11 \mod 24$</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>$(p-11)/24$</td>
</tr>
<tr>
<td>$p \equiv 13 \mod 24$</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>$(p-13)/24$</td>
</tr>
<tr>
<td>$p \equiv 17 \mod 24$</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>$(p-17)/24$</td>
</tr>
<tr>
<td>$p \equiv 19 \mod 24$</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>$(p-19)/24$</td>
</tr>
<tr>
<td>$p \equiv 23 \mod 24$</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>$(p+1)/24$</td>
</tr>
</tbody>
</table>

Moreover if the type is one or two, then the norm is one.

Let $K = \mathbb{Q}(\sqrt{D})$ be a real quadratic field over $\mathbb{Q}$ with a square-free rational integer $D$ and $O$ be the ring of integers in $K$. By $\text{gen}_L$ we denote the genus containing a lattice $L$ in a quadratic space $V$ over $K$. A lattice $L$ is said to be even if $Q(L) \subseteq 2O$. For vectors $x_1, \ldots, x_m$ in $V$, $[x_1, \ldots, x_m]$ denotes the lattice generated by $\{x_1, \ldots, x_m\}$ over $O$. 

4
Let \( \mathfrak{a} \) be a non-zero ideal of \( O \) and \( \mathcal{L} \) be a unimodular lattice in \( V \). For \( x \in \mathfrak{a}^{-1}\mathcal{L} \) such that \( Q(x) \in O \), we put
\[
\mathcal{L}(x) = 0x + \{ z \in \mathcal{L} : B(x,z) \in O \},
\]
which is called an \( \mathfrak{a} \)-adjacent lattice to \( \mathcal{L} \) (cf. [2]). The following Lemmas 1 - 4 are valid.

**Lemma 1.** Let \( \mathcal{L} \) be a unimodular lattice and \( \mathcal{L}(x) \) be an \( \mathfrak{a} \)-adjacent lattice to \( \mathcal{L} \). Then \( \mathcal{L}(x) \) is unimodular. If \( \mathfrak{a} \) is prime to 20 or \( \mathcal{L}(x)_\mathfrak{p} = \mathcal{L}_\mathfrak{p} \) for any dyadic spot \( \mathfrak{p} \), then an \( \mathfrak{a} \)-adjacent lattice to \( \mathcal{L} \) belongs to \( \text{gen}\mathcal{L} \).

**Lemma 2.** Let \( \mathcal{L} \) be a unimodular lattice in \( V \), and \( \mathcal{L}(x) \) and \( \mathcal{L}(x') \) be two \( \mathfrak{a} \)-adjacent lattices to \( \mathcal{L} \). If \( B(x,x') \in O \) and \( x - \gamma x' \in \mathcal{L} \) for some \( \gamma \in O \) prime to \( \mathfrak{a} \), then \( \mathcal{L}(x) = \mathcal{L}(x') \).

**Lemma 3.** Let \( \mathcal{L} \) be a unimodular lattice in \( V \) and \( \mathcal{L}(x) \) and \( \mathcal{L}(x') \) be two \( \mathfrak{a} \)-adjacent lattices to \( \mathcal{L} \). If \( x' = \sigma x \) for some \( \sigma \) in \( O(\mathcal{L}) \), then \( \mathcal{L}(x) = \mathcal{L}(x') \).

**Lemma 4.** Let \( \mathcal{L} \) be a unimodular lattice in \( V \) and \( \mathcal{L}(x) \) be an \( \mathfrak{a} \)-adjacent lattice to \( \mathcal{L} \). If there is a vector \( w \) in \( \mathcal{L} \) such that \( 2/Q(x-w) \) and \( (Q(x)-Q(w))/Q(x-w) \) are in \( \mathfrak{a} \), then \( \mathcal{L}(x) = \mathcal{L} \).

**Lemma 5.** Let \( p \) be an odd prime number dividing \( D \) and \( \mathfrak{p} \) a prime ideal dividing \( p \). Then a \( \mathfrak{p} \)-adjacent lattice to \( \mathcal{E}_n \) is isometric to some \( \mathcal{E}_n(x) \) with \( x = \sqrt{D} \sum_{i=1}^{n} a_i e_i \) and \( (a_1, \ldots, a_n) \in \mathbb{R}_n \cup \{(0, \ldots, 0)\} \).
Note that $pO = \mathfrak{p}^2$ and $O/\mathfrak{p} = \mathbb{Z}/p\mathbb{Z}$. Take an element $z = \sum_{i=1}^{n} \alpha_i e_i \in \mathfrak{p}^{-1}E_n$ with $Q(z) \in O$. We can find $a_i \in \mathbb{Z}$ such that $$\sqrt{D}a_i \equiv \frac{D}{p}a_i \mod \mathfrak{p}$$ since $\sqrt{D}a_i \in O$ and $\frac{D}{p}$ is prime to $\mathfrak{p}$. Put $x = \frac{D}{p} \sum_{i=1}^{n} a_i e_i$. Then $x \in \mathfrak{p}^{-1}E_n$ and $z - x \in E_n$. We have $\sum_{i=1}^{n} a_i^2 \equiv 0 \mod p$ since $Q(z) \in O$. Hence $Q(x) \equiv 0$ and $(a_1, \ldots, a_n) \in \mathbb{A}_p^n$ if $x \notin E_n$. Since $-2B(x, z) = Q(z - x) - Q(x) - Q(z) \equiv 0$ and $B(x, z) \in \mathfrak{p}^{-2}$, we have $B(x, z) \notin O$. By Lemma 2 we have $E_n(z) = E_n(x)$. Considering the structure of $O(E_n)$, we may have $(a_1, \ldots, a_n) \in \mathbb{R}_p^n \cup \{(0, \ldots, 0)\}$ by Lemmas 2 and 3.

§ 3. Special adjacent lattices to $E_n$.

Proposition 2. Let $b_1, \ldots, b_n$ be positive rational integers satisfying $\sum_{i=1}^{n} b_i^2 = D$. Assume $n \geq 3$. Consider the lattice $\mathbb{A} = E_n(\mathbb{Z}) = [z] \perp A$ with $z = \frac{1}{\sqrt{D}} \sum_{i=1}^{n} b_i e_i$. Then

1) $\mathbb{A} \in \text{gen } E_n$,

2) $A$ is even if $n \equiv b_1 \equiv \cdots \equiv b_n \equiv 1 \mod 2$,

3) $\mathbb{A} \in \text{gen } E_{n-1}$ unless $n \equiv b_1 \equiv \cdots \equiv b_n \equiv 1 \mod 2$,

4) $A = E_2$ if $n = 3, D \equiv 1 \mod 4$ and $b_i = b_j$ for some $i < j$,

5) $1 \not\in Q(A)$ unless $n = 3, D \equiv 1 \mod 4$ and $b_i = b_j$ for some $i < j$.

Proof. (i) Suppose that $D$ is odd. By Lemma 1 we have $\mathbb{A} \in \text{gen } E_n$. Let $\mathfrak{p}$ be a dyadic spot on $K$. We can assume that $b_1$ is odd. Put $v_i = b_1 e_i - b_i e_1$ for $i = 2, 3, \ldots, n$. Then $A_\mathfrak{p} = [v_2, \ldots, v_n]_\mathfrak{p}$ with $B(v_1, v_j) \in \mathbb{Z}$ and $\det(B(v_1, v_j)) = b_1^{2(n-2)}D \equiv 1 \mod 2$. The assertion (2) is clear. We shall show (3). Consider a lattice $M = [v_2, \ldots, v_n]$
over \( Z \). Then \( M_2 = <1> \perp \cdots \perp <1> \perp <D> \) or \( M_2 = <1> \perp <1> \perp <D> \perp <D> \perp <D> \). Since \( M \) is not even and the Hasse symbol of \( M_2 \) takes the value \(+1\), where \( M_2 \) is the 2\(^{\infty}\)-completion of \( M \). So \( A_\Phi = E_{n-1} \) since \( \Phi \subseteq \mathbb{Z}_2 \) and \( \sqrt{D} \in K \). By Lemma 1 we have the assertion (3).

(ii) Suppose that \( D \) is even. We can assume that \( b_1 \) and \( b_2 \) are odd. Let \( \Phi \) be dyadic. Then \( A_\Phi = [b_1 z - \sqrt{D} e_1, v_3, \ldots, v_n]_\Phi \) with \( \det(B(v_i, v_j)) = b_1^2(n-3)(D - b_2^2) \equiv 1 \mod 4 \). Thus \( A_\Phi = [v_3, \ldots, v_n]_\Phi \perp <D - b_2^2> \). By a similar argument as in (i) we have \( A_\Phi = E_{n-1} \). By Lemma 1 we have \( A \in \text{gen} E_{n-1} \), and so \( A \in \text{gen} E_n \).

(iii) Suppose that \( n = 3, D \equiv 1 \mod 4 \) and \( b_1 = b_2 \). Thus \( b_3 \equiv 1 \mod 2 \). Take \( f \) and \( g \) in \( Z \) such that \( 2b_2f - b_3g = 1 \). Put \( \omega_1 = -(b_3f + b_2g)z + f\sqrt{D}e_3 + \frac{1}{2}(1 + g\sqrt{D}) e_1 + \frac{1}{2}(-1 + g\sqrt{D}) e_2 \) and \( \omega_2 = \omega_1 - e_1 + e_2 \). Then \( A = [\omega_1] \perp [\omega_2] = E_2 \).

(iv) We shall show the assertion (5). Any non-zero vector \( u \in A \) can be written as \( u = -az + \sum_{i=1}^{n} (c_i + d_i \sqrt{D}) e_i \) with \( a = \sum_{i=1}^{n} b_i d_i \in Z \), \( \sum_{i=1}^{n} b_i c_i = 0 \), \( |a| \leq \frac{1}{2}D \), \( c_i \in \frac{1}{2}Z \), \( d_i \in \frac{1}{2}Z \) and \( c_i - d_i \in \frac{1}{2}Z \) for all \( i \). Thus

\[
Q(u) = \sum_{i=1}^{n} c_i^2 + D \sum_{i=1}^{n} d_i^2 - a^2 + 2\sqrt{D} \sum_{i=1}^{n} c_i d_i = \sum_{i=1}^{n} c_i^2 + \sum_{i<j}^{n} (b_i d_j - b_j d_i)^2 + 2\sqrt{D} \sum_{i=1}^{n} c_i d_i.
\]

If the number of the pairs \((i, j)\) such that \( b_i d_j - b_j d_i \neq 0 \) and \( i < j \) is less than \( n-1 \), then \( b_i d_j - b_j d_i = 0 \) for all \( i \) and \( j \). Hence \( d_i/b_i = \cdots = d_n/b_n = c \) for some \( c \in \mathbb{Q} \). Since the g.c.d. of \( b_i \)'s is one, we have \( c \in \frac{1}{2}Z \) or \( c \in Z \) according as \( D \equiv 1 \mod 4 \) or not.

Thus \( a = \sum_{i=1}^{n} b_i d_i = c \sum_{i=1}^{n} b_i^2 = cD \). This implies \( c = 0 \) and \( a = d_1 = \cdots = d_n = 0 \). Hence \( c_i \in \frac{1}{2}Z \) for all \( i \) and so \( \sum_{i=1}^{n} c_i^2 \geq 2 \). This shows \( Q(u) \neq 1 \). Suppose that the number of the pairs \((i, j)\) such that \( b_i d_j - b_j d_i \neq 0 \) and \( i < j \) is not less than \( n-1 \). If all \( d_i \)'s
are in $Z$, then $\sum_{i<j} (b_i d_j - b_j d_i)^2 \geq n-1 \geq 2$, so $Q(u) \neq 1$. Thus we may assume that $D \equiv 1 \mod 4$ and $d_i \notin Z$ for some $i$. Thus $c_i \notin Z$. Then $\sum_{i=1}^n c_i^2 = 2$ since $b_1 b_2 \cdots b_n \neq 0$. Hence

\[ \sum_{i=1}^n c_i^2 = \frac{1}{4} + \frac{1}{4}(n-1) = \frac{1}{4}(n+1) \geq 1 \]

and the equality holds only when $n = 3$ and $\sum_{i=1}^n c_i^2 = \frac{1}{4}$. This case occurs only when $n = 3$ and $b_i = b_j$ for some $i < j$ since $\sum_{i=1}^n b_i c_i = 0$. But this is excluded.

The following Lemma can be proved easily.

Lemma 6. Let $D$ be a square-free positive integer. In order that $D = b_1^2 + b_2^2 + b_3^2 + b_4^2$ for some positive integers $b_1, b_2, b_3$ and $b_4$, it is necessary and sufficient that $D \not\equiv 1, 2, 3, 5, 6, 11, 14, 17, 29, 41$. 

Proposition 3. Let $D \equiv l \mod 4$. Let $p$ be an odd prime dividing $D$. Consider the lattice $B = E_3(y)$ with $y = \frac{\sqrt{D}}{p} \sum_{i=1}^3 a_i e_i$ and $(a_1, a_2, a_3) \in R_p^3$. Then

1. $B \in \text{gen } E_3$,
2. $B = E_1 \perp E'$ and $1 \not\in Q(B')$ if $D = p = \sum_{i=1}^3 a_i^2$ or if $T(a_1, a_2, a_3) = 1$,
3. $1 \not\in Q(B)$ if $T(a_1, a_2, a_3) \geq 2$ and unless $D = p = \sum_{i=1}^3 a_i^2$.

Proof. By Lemma 1 we have $B \in \text{gen } E_3$. Suppose that $T(a_1, a_2, a_3) \geq 2$ and $Q(u) = 1$ for some $u \in B$. We can write $u = ay + \sum_{i=1}^3 (c_i + d_i \sqrt{D})e_i$ where $a \in Z, c_i \in Z, d_i \in Z, \sum_{i=1}^3 a_i c_i \equiv 0 \mod p$ and $|a| < \frac{1}{2} p$. 

Then
\[ Q(u) = \sum_{i=1}^{3} c_i^2 + \frac{3}{p} \sum_{i=1}^{3} (a_i + pd_i) + \frac{2\sqrt{D}}{p} \sum_{i=1}^{3} c_i(a_i + pd_i). \]

Hence we have \( \frac{3}{p} \sum_{i=1}^{3} c_i^2 = 0 \) and \( D = p \sum_{i=1}^{3} (a_i + pd_i)^2 \) since \( T(a_1, a_2, a_3) \geq 2. \)

Thus the assertion (3) holds. Now let \( D = p \sum_{i=1}^{3} a_i^2. \) Then \( B = \langle y \rangle \perp B' \) and \( Q(B') \neq 1 \) by (5) of the Proposition 2. If \( T(a_1, a_2, a_3) = 1, \) then \( a_1 = 0, D \neq p \) and \( B = [e_1] \perp B'. \) Similarly we have \( 1 \notin Q(B'). \)

Proposition 4. Let \( D \equiv 1 \) mod 4 and \( p \) be a prime dividing \( D. \) Consider the lattice \( B = E_n(y) \) with \( y = \frac{\sqrt{D}}{p} \sum_{i=1}^{n} a_i e_i \) and \( (a_1, \ldots, a_n) \in \mathbb{R}^n_p. \) Assume that \( n \geq 3. \) Put \( T = T(a_1, \ldots, a_n) \) and \( N = N(a_1, \ldots, a_n). \)

Then

1. \( B \in \text{gen} E_n, \)
2. \( B = E_1 \perp B' \) with \( 1 \notin Q(B') \) if \( n = 3, D \neq p \) and \( T = 1. \)
3. \( 1 \notin Q(B) \) and \( 2 \in Q(B) \) if \( D \neq p \) and \( T = 2, \)
4. \( 1 \notin Q(B) \) and \( 2 \notin Q(B) \) if \( D \neq p \) and \( T \geq 3, \)
5. \( B = E_3 \) if \( n = 3, D = p \) and \( T \leq 2, \)
6. \( B = E_1 \perp B' \) with \( 1 \notin Q(B') \) if \( D = p, N = 1 \) and \( T \geq 3, \)
7. \( 1 \notin Q(B) \) if \( D = p, N = 2 \) and \( T \geq 3, \)
8. \( 1 \notin Q(B) \) if \( D = p, N \geq 3 \) and \( T \geq 2, \)
9. \( 2 \notin Q(B) \) if \( n = 3, D = p, N \geq 3 \) and \( T \geq 3, \)
10. \( 2 \in Q(B) \) if \( D = p \) with \( N = 2 \) or if \( T = 2. \)

Proof. By Lemma 1 we have (1). (10) holds trivially. Take a non-zero vector \( u \) in \( B \) and write
\[ u = ay + \sum_{i=1}^{n} (c_i + d_i \sqrt{D}) e_i \]
with \( a \in \mathbb{Z}, |a| < \frac{1}{2}p, c_i \in \frac{1}{2} \mathbb{Z}, d_i \in \frac{1}{2} \mathbb{Z}, c_i - d_i \in \mathbb{Z} \) and \( 2 \sum_{i=1}^{n} a_i c_i \equiv 0 \) \( \text{mod} \ p. \) Then
\[ Q(u) = X + Y + \frac{2\sqrt{D}}{p} \sum_{i=1}^{n} c_i(a_i + pd_i). \]
where $X = \sum_{i=1}^{n} c_i^2$ and $Y = \frac{D}{p} \sum_{i=1}^{n} (a_i + pd_i)^2$. If $Y = 0$, then $a_i = 0$ for all $i$, so $c_i \in \mathbb{Z}$ for all $i$. Thus $X \geq T$. If $X = 0$ and $Y \neq 0$, then $c_i = 0$ for all $i$ and $Y \geq DN/p$. Thus $X \geq 0$ and $Y < 0$, then $X + Y \geq \frac{T}{4} + \frac{DN}{p^2}$. Thus $(3),(7),(8)$ and the half of $(4)$ hold. Now suppose that $D \neq p$ and $T \geq 2$ or that $D = p$, $T \geq 3$, $N \geq 3$ and $n = 3$. Thus $X \geq 3/4$ and $Y \geq 3/4$. If $X = 3/4$ with $Y = 5/4$, we have $2 = 4X - 4Y \leq \sum_{i=1}^{n} (2c_i)^2 - i_{11}(2d_i)^2 \equiv 0 \mod 4$, which is a contradiction. If $X = Y = 1$, then $D = p$ and $n \geq 4$, which is a contradiction. Hence $(9)$ and the rest of $(4)$ hold. If $n = 3$, $D \neq p$ and $T = 1$, then $a_i = 0$ and $B = [e_1] \perp B'$ with $B' = [e_2, e_3](y)$. Hence we have $1 \notin Q(B')$ by a direct calculation. So the assertion $(2)$ holds. Assume that $n = 3$, $D = p$ and $T \leq 2$. Then $N = 1$. If $T = 1$, then $B = [e_1] \perp [y] \perp [y'] = E_3$ with $y' = \frac{1}{\sqrt{p}}(a_3 e_2 - a_2 e_3)$. If $T = 2$, then $B = E_3$ by Proposition 2,(4). Thus $(5)$ holds. Finally $(6)$ follows from Proposition 2,(5).

Proposition 5. Let $D \equiv 3 \mod 4$. Consider the lattice $C = E_3(x) = [e_3] \perp C'$ with $x = \frac{1}{\sqrt{p}}(e_1 + \sqrt{D} e_2)$. Then

1. $C \in \text{gen } E_3$,
2. $1 \notin Q(C')$ if $D > 3$,
3. $C'$ is even if and only if $D \equiv 7 \mod 8$.

Proof. We have $C' = [x, 2 e_2] = \{\frac{1}{\sqrt{D}} \frac{D+1}{\sqrt{D}} \}_{D=4}$. Let $p$ be dyadic.

If $D \equiv 3 \mod 8$, then $C'$ is not even and $C'_p = <\frac{1}{\sqrt{D}}(D+1)> \perp <\frac{1}{\sqrt{D}}(D+1)> = E_2 \perp$ since $3 \notin K^2_p$. If $D \equiv 7 \mod 8$, then $C'$ is even and $C'_p = [0, 1]$ and $C'_p = <\frac{1}{\sqrt{D}}(D+1)> \perp <\frac{1}{\sqrt{D}}(D+1)> = E_3 \perp$ since $-1 \notin K^2_p$. Thus (1) and (3) are proved by Lemma 1. It is easy to show (2) directly.
Proposition 6. Let $D \equiv 5 \mod 12$. Consider the lattice \( G = E_3(x) = \mathbb{Z}G^t \) with \( x = \frac{1}{3}(e_1 + D\sqrt{D}e_2) \). Then

1. \( G \in \text{gen} E_3 \) and \( G' \in \text{gen} E_2 \),
2. \( 1 \notin Q(G') \) and \( 2 \notin Q(G') \) if \( D \geq 29 \).

Proof. (1) follows from Lemma 1. We have \( G' = [x, 3e_2] \). It is easy to show (2) by a direct calculation.

Proposition 7. Let \( D \) be a prime \( p \equiv 1 \mod 12 \). Then the number of the classes in \( A_3^p \) whose type is six is one or zero according as \( p \equiv 1 \mod 24 \) or \( p \equiv 13 \mod 24 \). Let \( (a_1, a_2, a_3) \in \mathbb{R}_3^p \) with \( T = T(a_1, a_2, a_3) \geq 3 \) and \( N(a_1, a_2, a_3) = 2 \). Put \( x = \frac{1}{\sqrt{p}}(a_1e_1 + a_2e_2 + a_3e_3) \). If there are two vectors \( u_1 \) and \( u_2 \) in \( B = E_3(x) \) such that \( Q(u_1) = Q(u_2) = 2B(u_1, u_2) = 2 \), then \( T = 3 \) or \( T = 6 \).

Proof. Let \( (b_1, b_2, b_3) \in A_3^p \) whose type is six. Thus we may assume that \( b_3 = 2b_1 + b_2 \). Hence \( 0 \equiv \sum_{i=1}^{3} b_i^2 = 2(b_1 + b_2)^2 + 3b_1^2 \mod p \). So

\[
\left( \frac{-6}{p} \right) = 1, \text{ i.e., } p \equiv 1 \mod 24. \quad \text{If } p \equiv 1 \mod 24, \text{ then there is an integer } c \text{ such that } c^2 \equiv -6 \mod p. \quad \text{Hence } \pm c(b_1 + b_2) \equiv 3b_1 \mod p.
\]

Thus \( (b_1, b_2, b_3) \sim (c, 3-c, 3+c) \), i.e., there is one and only one class whose type is six. We shall show \( T = 3 \) or \( T = 6 \). Suppose that \( T \neq 3 \) and \( T \neq 6 \). Thus \( T = 5 \) or \( T \geq 7 \). Take a vector \( u \) in \( B \) with \( Q(u) = 2 \) and write

\[
u = ax + \sum_{i=1}^{3} (c_i + d_i \sqrt{p})e_i
\]

with \( a \in \mathbb{Z}, \ |a| < \frac{1}{3}p, \ c_i \in \frac{1}{2}\mathbb{Z}, \ d_i \in \frac{1}{2}\mathbb{Z}, \ c_i - d_i \in \mathbb{Z}, \ 2 \sum_{i=1}^{3} a_i c_i = 0 \mod p.
\]

Then \( Q(u) = X + Y + \frac{2}{\sqrt{p}} \sum_{i=1}^{3} c_i (a a_i + p d_i) \), where \( X = \sum_{i=1}^{3} c_i^2 \) and \( Y = \).
\[
\frac{1}{3} \sum_{i=1}^{3} (a_{a_i} + p d_i)^2. \quad \text{Hence we have one of the following:}
\]

(i) \(X = 0\) and \(Y = 2\),

(ii) \(X = 5/4\) and \(Y = 3/4\),

(iii) \(X = 3/2\) and \(Y = 1/2\).

In the case (ii) we have
\[
1 = \frac{3}{2} (2c_1)^2 = \frac{3}{2} (2d_1)^2 = \frac{3}{2} (2a_{a_1} + 2pd_1)^2
\]

\[= 3p \equiv 3 \mod 4. \text{ This is a contradiction. In the case (iii) we have}\]
\[(a_1, a_2, a_3) \sim (c, 3-c, 3+c) \text{ for an integer } c \text{ with } c^2 + 6 \equiv 0 \mod p \text{ by the argument used above since } X = 6/4. \text{ Since } T \text{ must be five we have } c \equiv \pm 1, \pm 2, \pm 3, \pm 6 \text{ or } \pm 9 \mod p, \text{ which is a contradiction to the fact that } p \text{ divides } c^2 + 6. \text{ In the case (i) we have } c_i = 0 \text{ and } d_i \in \mathbb{Z} \text{ for all } i. \text{ Hence we can write } u_1 = ax + \sqrt{p} \sum_{i=1}^{3} d_i e_i = \frac{1}{\sqrt{p}} \sum_{i=1}^{3} f_i e_i \text{ and } u_2 = a'x + \sqrt{p} \sum_{i=1}^{3} d_i' e_i = \frac{1}{\sqrt{p}} \sum_{i=1}^{3} f_i' e_i
\]

with \(a, a', d_i, d_i', f_i, f_i' \in \mathbb{Z}\). Thus \(f_i \equiv a_{a_i} \mod p\) and \(f_i' \equiv a'_{a_i} \mod p\). Hence \(f_i f_i' - f_j f_j' \equiv 0 \mod p\). Since \(3p^2 = (2p)^2 - p^2 = \sum_{i=1}^{3} f_i^2 \sum_{j=1}^{3} f_j^2 - (\sum_{i=1}^{3} f_i f_i')^2 = \sum_{i \neq j} (f_i f_i' - f_j f_j')^2 \), we have \(f_i f_i' - f_j f_j' = h_{ij} \) \(\equiv \pm p \text{ whenever } i \neq j\). Since \(0 = f_1 (f_2 f_3^* - f_3 f_2^*) + f_2 (f_3 f_1^* - f_1 f_3^*) + f_3 (f_1 f_2^* - f_2 f_1^*)\), we have \(0 = f_1 h_{23} + f_2 h_{31} + f_3 h_{12}\), i.e., \(a_1 h_{23} + a_2 h_{31} + a_3 h_{12} \equiv 0 \mod p\). This implies that \(T \leq 3\). This is a contradiction.

Proposition 8. Let \(n \geq 3\). Then the class number of \(E_n\) is more than two unless \(D\) is one of the following: 2, 3, 5, 13, 17, 29, 33, 41.

Proof. It is enough to find two lattices \(L\) and \(M\) in \(\text{gen } E_3\) such that \(L \neq E_3, M \neq E_3\) and \(L \neq M\).
(i) Let $D \equiv 2 \mod 4$. For $L$ we take the lattice $A$ in the Proposition 2 if $D = 10$. If $D \neq 10$, then there is an odd prime $q$ $(\neq 5)$ dividing $D$. By the Proposition 1 there is an element $(a_1, a_2, a_3) \in \mathbb{R}_q^3$ whose type is more than one, for which we consider the lattice $B$ in the Proposition 3. Then put $L = B$ if $D \neq 10$.

Next take an odd prime $p$ dividing $D$. If $p \equiv 1 \mod 4$, then there is an element $(a_1, a_2, a_3) \in \mathbb{R}_p^3$ whose type is one, for which we consider the lattice $B$ in the Proposition 3. If $p \equiv 3 \mod 4$, then we can consider the lattice $\overline{A}$ in the Proposition 2. Then put $M = B$ or $M = \overline{A}$ according as $p \equiv 1 \mod 4$ or $p \equiv 3 \mod 4$. Note that $1 \notin Q(L)$ and $M = E_1 \perp M'$ with $1 \notin Q(M')$.

(ii) Let $D \equiv 3 \mod 8$. For $L$ we take a lattice $\overline{A} = E_1 \perp A$ with an even lattice $A$ in the Proposition 2. For $M$ we take the lattice $C = E_1 \perp C'$ with an odd lattice $C'$ and $1 \notin Q(C')$ in the Proposition 5.

(iii) Let $D \equiv 7 \mod 8$. For $L$ we take a lattice $A$ with $1 \notin Q(A)$ in the Proposition 2 and for $M$ we take the lattice $C = E_1 \perp C'$ with $1 \notin Q(C')$ in the Proposition 5.

(iv) Let $D \equiv 1 \mod 4$ and not a prime. If no prime divisor of $D$ is congruent to $7 \mod 8$, then by the Proposition 1 we have two elements $(a_1, a_2, a_3) \in \mathbb{R}_p^3$ and $(a'_1, a'_2, a'_3) \in \mathbb{R}_q^3$ for some prime divisors $p$ and $q$ of $D$ (possibly $p = q$) such that $T(a_1, a_2, a_3) = 1$ and $T(a'_1, a'_2, a'_3) \geq 2$ or such that $T(a_1, a_2, a_3) = 2$ and $T(a'_1, a'_2, a'_3) \geq 3$. For $L$ and $M$ we take the lattice $B$ for $(a_1, a_2, a_3)$ and the lattice $B$ for $(a'_1, a'_2, a'_3)$ in the Proposition 4. If $D$ has a prime divisor $p \equiv 7 \mod 8$, then there is an element $(a_1, a_2, a_3) \in \mathbb{R}_p^3$ whose type is more than two, for which we can consider the lattice $B$ with $Q(B) \neq 1$ in the Proposition 4. Put
There are positive integers $b_1, b_2$ and $b_3$ such that $b_1^2 + b_2^2 + b_3^2 = D$ since $D \equiv 1 \mod 4$ and $p \equiv 3 \mod 4$. We have $b_i \neq b_j$ whenever $i \neq j$ since $(-\frac{2}{p}) = -1$. Hence we can consider a lattice $\mathcal{A} = \mathbb{E}_1 \perp \mathcal{A}$ with $1 \notin Q(\mathcal{A})$. Put $M = \mathcal{A}$.

(v) Let $D$ be a prime $p \equiv 1 \mod 12$. Since $p = 3a^2 + b^2$ for some positive integers $a$ and $b$, we can consider the lattice $\mathcal{A}$ for $(a, a, a, b)$ in the Proposition 2. Put $L = \mathcal{A}$. Then $1 \notin Q(L)$ and there are two vectors $u_1$ and $u_2$ in $L$ such that $Q(u_1) = Q(u_2) = 2B(u_1, u_2) = 2$. First suppose $p \equiv 1 \mod 24$. Then there are at least two elements $(a_1, a_2, a_3)$ and $(a_4, a_2, a_3)$ in $\mathbb{R}_p^3$ whose types are more than three by Proposition 1. Hence we can assume that $T(a_1, a_2, a_3) \neq 6$ by Proposition 7. We put $M = 8$ for $(a_1, a_2, a_3)$ in Proposition 4. Hence $M \notin \mathcal{E}_3$. And $M \notin L$ if $N(a_1, a_2, a_3) \neq 2$. If $M = L$ and $N(a_1, a_2, a_3) = 2$, then (noting the existence of the pair $(u_1, u_2)$) we have $T(a_1, a_2, a_3) = 3$ or $6$ by Proposition 7. This is a contradiction. Secondly suppose that $p \equiv 13 \mod 24$. There is an element $(a_1, a_2, a_3) \in \mathbb{R}_p^3$ whose type is more than three by the Proposition 1. For $M$ we take the lattice $L$ for $(a_1, a_2, a_3)$ in the Proposition 4.

If $N(a_1, a_2, a_3) = 1$, then $B = \mathbb{E}_1 \perp B'$ with $1 \notin Q(B')$. If $N(a_1, a_2, a_3) \geq 3$, then $1 \notin Q(B)$ and $2 \notin Q(B)$. If $N(a_1, a_2, a_3) = 2$, then $1 \notin Q(B)$ and $B \notin L$ by Proposition 7.

(vi) Let $D$ be a prime $p \equiv 5 \mod 12$. For $L$ we take the lattice $\mathcal{A}$ with $1 \notin Q(\mathcal{A})$ in Proposition 2. For $M$ we take the lattice $G = \mathbb{E}_1 \perp G'$ with $1 \notin Q(G')$ in Proposition 6.
§ 4. Special values of $D$. For the explicit value of the class number of $E_n$, we use the Kneser Method. Following [4], we state the method. By $J$ we denote the group of ideles of the field $K$.

For a finite spot $\mathfrak{p}$ on $K$ we put

$$J^\mathfrak{p} = \{ i = (i_{\mathfrak{q}}) \in J ; \ i_{\mathfrak{q}} \text{ is a unit in } O_{\mathfrak{q}} \text{ for all finite spot } \mathfrak{q} \neq \mathfrak{p} \}.$$  

Put $V = KE_n$ and $P = \Theta(O^+(V))$, where $\Theta$ is the spinor norm and $O^+(V)$ is the proper orthogonal group of $V$. Consider $P$ as the image of $P$ under the natural isomorphism $K^* \to J$. Recall Lemma 10 of [4] in [4]:

Lemma 7. Let $n \geq 3$, $V_\mathfrak{p}$ be isotropic and $J = PJ^\mathfrak{p}$. Then for any $L \in \text{gen } E_n$, there is a lattice $M$ isometric to $L$ such that $M_\mathfrak{q} = E_n \mathfrak{q}_L$ for all finite spot $\mathfrak{q} \neq \mathfrak{p}$.

By the Proposition 101:8 in [4], we have

Lemma 8. Let $n \geq 3$ and the ideal class number of $K$ be one. Assume that the norm of the fundamental unit in $K$ is $\pm 1$ or that the norm of a generator of $\mathfrak{p}$ is negative. Then $J = PJ^\mathfrak{p}$.

Lemma 9. Let $n \geq 3$, $\mathfrak{p}$ be a spot dividing $D$ and $M \in \text{gen } E_n$ with $M_\mathfrak{q} = E_n \mathfrak{q}_M$ for all finite spot $\mathfrak{q} \neq \mathfrak{p}$. Assume that $n$ is odd and $D = 2$ if $\mathfrak{p}$ is dyadic. Then there is a chain of lattices $E_n = L_0, L_1, \ldots, L_t = M$ in $\text{gen } E_n$ with $L_{i+1} \mathfrak{p}$-adjacent to $L_i$.

Proof. Following the proof of 106:4 in [4], we can prove this assertion. It is enough to find a chain of lattices $E_n \mathfrak{p} = L_0(\mathfrak{p}), L_1(\mathfrak{p}), \ldots, L_t(\mathfrak{p}) = M_\mathfrak{p}$ in $V_\mathfrak{p}$ with $L_i(\mathfrak{p}) \mathfrak{p}$-adjacent to $L_{i+1}(\mathfrak{p})$ and $L_1(\mathfrak{p}) = E_n \mathfrak{p}$. Put $L_0 = E_n$. Then $M_\mathfrak{p} = \sigma L_0(\mathfrak{p})$ for some $\sigma \in O(V_\mathfrak{p})$. By
expressing \( \sigma \) as a product of symmetries on \( V_6 \) we see that it is enough if we assume that \( \sigma \) is a symmetry. Then \( \sigma = \tau_u \) with \( u \) a maximal anisotropic vector in \( L_0 \). Then there is either a 1- or 2-dimensional unimodular sublattice \( K \) of \( L_0 \) which contains \( u \).

If the rank of \( K \) is one, then \( L_0 = \tau_u L_0 = M_0 \), so \( M_0 \) is \( \sigma \)-adjacent to \( L_0 \). If the rank of \( K \) is two, then we take the splitting \( L_0 = K \perp K' \). Then \( K' = \tau_u K \subset M_0 \) and so we have a splitting \( M_0 = K'' \perp K' \).

Write \( K = \mathbb{Z} \alpha + O_6 \) and \( K'' = O_6 \alpha + \mathbb{Z} \beta \) with a non-negative integer \( \beta \). Hence we may put \( L_0(\mathbb{Z}) = L_0 \), \( L_1(\mathbb{Z}) = (1 + \mathbb{Z} \beta) \perp K' = L_0(\mathbb{Z}(\mathbb{Z}-1)) \), \( \ldots \).

It is trivial that \( i = 0 \) or \( i = r \). Assume that \( 1 \leq i \leq r-1 \). If \( \beta \) is non-dyadic, then \( \mathbb{Z}(\mathbb{Z}-1) \perp K' = (O_6 \alpha + \mathbb{Z} \beta) \perp K' \), where \( \mathbb{Z} = \pi O_6 \). We must show that \( L_i(\mathbb{Z}) = \mathbb{Z} \). Write \( K = \mathbb{Z} \alpha + O_6 \) and \( K'' = O_6 \alpha + \mathbb{Z} \beta \) with a non-negative integer \( \beta \). Hence we may put \( L_0(\mathbb{Z}) = L_0 \), \( L_1(\mathbb{Z}) = (1 + \mathbb{Z} \beta) \perp K' = L_0(\mathbb{Z}(\mathbb{Z}-1)) \), \( \ldots \).

It is trivial that \( i = 0 \) or \( i = r \). Assume that \( 1 \leq i \leq r-1 \). If \( \beta \) is non-dyadic, then \( \mathbb{Z}(\mathbb{Z}-1) \perp K' = (O_6 \alpha + \mathbb{Z} \beta) \perp K' \), where \( \mathbb{Z} = \pi O_6 \). We must show that \( L_i(\mathbb{Z}) = \mathbb{Z} \). It is trivial that \( i = 0 \) or \( i = r \). Assume that \( 1 \leq i \leq r-1 \). If \( \beta \) is non-dyadic, then \( \mathbb{Z}(\mathbb{Z}-1) \perp K' = (O_6 \alpha + \mathbb{Z} \beta) \perp K' \), where \( \mathbb{Z} = \pi O_6 \). We must show that \( L_i(\mathbb{Z}) = \mathbb{Z} \). It is trivial that \( i = 0 \) or \( i = r \). Assume that \( 1 \leq i \leq r-1 \). If \( \beta \) is non-dyadic, then \( \mathbb{Z}(\mathbb{Z}-1) \perp K' = (O_6 \alpha + \mathbb{Z} \beta) \perp K' \), where \( \mathbb{Z} = \pi O_6 \). We must show that \( L_i(\mathbb{Z}) = \mathbb{Z} \). It is trivial that \( i = 0 \) or \( i = r \). Assume that \( 1 \leq i \leq r-1 \). If \( \beta \) is non-dyadic, then \( \mathbb{Z}(\mathbb{Z}-1) \perp K' = (O_6 \alpha + \mathbb{Z} \beta) \perp K' \), where \( \mathbb{Z} = \pi O_6 \). We must show that \( L_i(\mathbb{Z}) = \mathbb{Z} \). It is trivial that \( i = 0 \) or \( i = r \). Assume that \( 1 \leq i \leq r-1 \). If \( \beta \) is non-dyadic, then \( \mathbb{Z}(\mathbb{Z}-1) \perp K' = (O_6 \alpha + \mathbb{Z} \beta) \perp K' \), where \( \mathbb{Z} = \pi O_6 \). We must show that \( L_i(\mathbb{Z}) = \mathbb{Z} \).

If \( Q(y) \equiv 0 \mod 2 \), then \( \mathbb{Z}(\mathbb{Z}-1) \perp K' = (O_6 \alpha + \mathbb{Z} \beta) \perp K' \), where \( \mathbb{Z} = \pi O_6 \). We must show that \( L_i(\mathbb{Z}) = \mathbb{Z} \).

If \( D = 2 \). Then the class number of \( \mathbb{Z} \) is one if \( n \leq 4 \), two if \( n = 5 \) and more than two if \( n \geq 6 \).
Proof. There are three lattices \( E_6, E_6(\frac{1}{\sqrt{2}}(e_1+\cdots+e_6)), \) and \( E_6(\frac{1}{\sqrt{2}}(e_1+\cdots+e_6)) \) in \( \text{gen} E_6 \), any two of which are not isometric.

Let \( n = 5 \). Take \( \mathfrak{g} = (\sqrt{2}) \) and a \( \mathfrak{g} \)-adjacent lattice \( E_5(x) \) in \( \text{gen} E_5 \). Write \( x = \frac{1}{\sqrt{2}} \sum_{i=1}^{5} a_i e_i \). Note that \( O(E_5) \) contains all permutations of \( \{e_1, \ldots, e_5\} \). And note that \( Q(x) \equiv 0 \) or \( 1 \) mod 2 since \( E_5(x) \in \text{gen} E_5 \). By Lemmas 2 and 3 we have only to consider the following three cases: (i) \( a_1 = a_2 = a_3 = a_4 = a_5 = 0 \). Then \( E_5(x) = E_5 \). (ii) \( a_1 = a_2 = 1 \) and \( a_3 = a_4 = a_5 = 0 \). Then \( E_5(x) = E_5 \). (iii) \( a_1 = a_2 = a_3 = a_4 = 1 \) and \( a_5 = 0 \). Then \( E_5(x) = E_5^0 \). Where \( E_4 = E_4(u) \) with \( u = \frac{1}{\sqrt{2}}(e_1+\cdots+e_4) \). Hence a \( \mathfrak{g} \)-adjacent lattice to \( E_5 \) in \( \text{gen} E_5 \) is isometric to \( E_5 \) or \( E_5^0 = E_4 \perp [e_5] \). Next take a \( \mathfrak{g} \)-adjacent lattice \( E_5(y) \) to \( E_5 \) in \( \text{gen} E_5 \) and write \( \sqrt{2} y = w + \alpha e_5 \) with \( \alpha \in \langle 0 \rangle \) and \( w \in E_4^0 \). Since \( Q(y) \equiv 0 \) and \( E_4^0 \) is even, we have \( \alpha \in \mathfrak{g} \). By Lemma 2 we have \( E_5^0(y) = E_5^0(\frac{1}{\sqrt{2}} w) = E_4^0(\frac{1}{\sqrt{2}} w) \perp [e_5] \).

Hence we may write \( \sqrt{2} y = a u + \sum_{i=1}^{4} a_ie_i \) where \( a_i \in \langle 0 \rangle \), \( a \in \{0, 1\} \) and \( \sum_{i=1}^{4} a_i \equiv 0 \) mod \( \sqrt{2} \). Note that \( Q(y) \equiv 0 \) or \( 1 \) mod \( 2 \) since \( E_5(y) \in \text{gen} E_5 \). If \( a = 0 \), then we have the following four cases by Lemmas 2 and 3: (i) \( a_1 = a_2 = a_3 = a_4 = 0 \). Then \( E_5^0(y) = E_5^0 \). (ii) \( a_1 = \sqrt{2} \) and \( a_2 = a_3 = a_4 = 0 \). Then \( E_5^0(y) = E_5 \). (iii) \( a_1 = a_2 = 1 \) and \( a_3 = a_4 = 0 \). Then \( E_5^0(y) = E_5 \). (iv) \( a_1 = a_2 = 1 \), \( a_3 = \sqrt{2} \) and \( a_4 = 0 \). Then \( E_5^0(y) = E_5 \). Next consider the case of \( a = 1 \). Since \( \tau_{e_1} \in O(E_4^0) \), we have \( \sqrt{2} y \tau_{e_1} = u + (-\alpha_1-\sqrt{2})e_1 + a_2 e_2 + \cdots \). Hence we may assume that \( a_i \equiv 0 \) mod \( 2 \) or \( a_i \equiv 1 \) mod \( 2 \). Thus we have only to consider the following cases by Lemmas 2 and 3: (v) \( a_1 = a_2 = a_3 = a_4 = 0 \) or \( a_1 = a_2 = a_3 = a_4 = 0 \). Then \( E_5^0(y) = E_5 \). (vi) \( a_1 = -1 \), \( a_2 = 1 \) and \( a_3 = a_4 = 0 \). Apply Lemma 4 to this case taking \( w = u - \sqrt{2} e_1 \). Then \( E_5^0(y) = E_4^0 \perp [e_5] \).
= E_5^1. Thus a $\mathcal{P}$-adjacent lattice to $E_5^1$ is isometric to $E_5$ or $E_5^1$. Hence \{E_5^1, E_5\} is a set of all representatives of classes in gen $E_5$ by Lemmas 7, 8 and 9. By Theorem 105:1 in [4] this implies that the class number is one if $n \leq 4$.

From [11] we have

**Proposition 10.** Let $D = 3$. Then the class number of $E_n$ is one if $n \leq 2$, two if $n = 3$ and more than two if $n \geq 4$.

**Proposition 11.** Let $D = 5$. Then the class number of $E_n$ is one if $n \leq 4$, two if $n = 5$ and more than two if $n \geq 6$.

**Proof.** Put $x = \frac{1}{\sqrt{5}}(e_1 + \cdots + e_5)$, $y_1 = \frac{1}{\sqrt{5}}(e_1 + 2e_2 + 2e_3 + 2e_4)$ and $x_1 = \frac{1}{\sqrt{5}}(e_1 + 2e_2 + 2e_4 + 2e_5 + 2e_6)$. Consider the lattice $E_5^1 = E_5(x) = [x] \perp E_4^0$. Then $E_4^0$ is even. If $n = 6$, then we have three lattices $E_6, E_6(x)$ and $E_6^1 = E_6(x_1)$ in gen $E_6$. By Proposition 4, (8) we have $1 \not\in \mathbb{Q}(E_6^1)$. Thus the class number of $E_6$ is more than two.

Let $\mathcal{P} = (\sqrt{5})$ and $n = 5$. Take a $\mathcal{P}$-adjacent lattice $E_5(y)$ to $E_5$.

By Lemma 5 we may consider $y = \frac{1}{\sqrt{5}} \sum_{i=1}^{5} a_i e_i$ with $(a_1, \ldots, a_5) \in \mathbb{R}_5^5$.

Hence $y \in \{0, x, \frac{1}{\sqrt{5}}(e_1 + 2e_2), y_1\}$. Thus $E_5(0) = E_5$, $E_5(x) = E_5^1$ and $E_5((\frac{1}{\sqrt{5}}(e_1 + 2e_2))) = E_5^1$. By the Lemma 4 $E_5(y_1) = E_5$ taking $w = \frac{1}{2}(1+\sqrt{5})(e_3 + e_4) \in E_5$. Take a $\mathcal{P}$-adjacent lattice $E_5^1(z)$ to $E_5^1$.

By Lemma 2 we may assume that $\sqrt{5} z = a x + \sum_{i=1}^{5} b_i e_i$ where $a = 0$ or 1, $a_i = a_i + b_i \sqrt{5} \in \mathbb{Z}[\sqrt{5}]$ and $\sum_{i=1}^{5} a_i \equiv 0 \mod 5$. If $a = 0$, then we have only to consider the following three cases by Lemmas 2 and 3:

(i) $a_1 = \cdots = a_5 = 0$. Then $z = \sum_{i=1}^{5} b_i e_i$, so $E_5^1(z) = E_5^1$ or $E_5^1(z) = E_5$ according as $\sum_{i=1}^{5} b_i \equiv 0 \mod 5$ or not.
(ii) $a_1 = \cdots = a_5 = 1$. Thus $z = x + \frac{5}{2} b_1 e_1$ with $\frac{5}{2} b_1 \equiv 0 \mod 5$, so $z \in E_5^1$. Hence $E_5^1(z) = E_5^1$.

(iii) $a_1 = 1$, $a_2 = -1$, $a_3 = 2$, $a_4 = -2$, $a_5 = b_1 = \cdots = b_4 = 0$ and $b_5 \in \{0,1\}$. If $b_5 = 0$, then $z \in E_5^1$, so $E_5^1(z) = E_5^1$. If $b_5 = 1$, then we have $E_5^1(z) = \left[ z_0, z_1, \ldots, z_4 \right] = E_5$, where $z_0 = z + \zeta e_3 + \zeta e_4 - e_5$, $z_1 = z + x + \zeta e_1 + \zeta e_3 - e_5$, $z_2 = z + 2x + \zeta e_1 - \sqrt{5} e_3 - \zeta e_5$, $z_3 = z - 2x + \zeta e_2 + \sqrt{5} e_4 - \zeta e_5$ and $z_4 = z - x + \zeta e_2 + \zeta e_4 - e_5$, where $\zeta = \frac{\sqrt{5} + 1}{2}$.

If $a = 1$, then we have only to consider the following six cases by Lemma 2 (note that $0(E_5^1)$ contains all permutations of $\{e_1, \ldots, e_5\}$):

(iv) $a_1 = \cdots = a_4 = 0$ and $a_5 = 2\sqrt{5}$. Thus $E_5^1(z) = \left[ 2z - 5e_5, 2z - e_1 - 4e_5, 2z - e_2 - 4e_5, 2z - e_3 - 4e_5, 2z - e_4 - 4e_5 \right] = E_5$.

(v) $a_1 = a_2 = a_3 = 0$, $a_4 = 2$ and $a_5 = 3 + 3\sqrt{5}$. Thus $E_5^1(z) = \left[ z + 2x - \zeta e_4 - (3 + \sqrt{5}) e_5, z - 2x - \zeta (e_1 + e_2 + e_3) - (3 + \sqrt{5}) e_5, z - e_1 - \zeta e_4 - (3 + \sqrt{5}) e_5, z - e_2 - \zeta e_4 - (3 + \sqrt{5}) e_5, z - e_3 - \zeta e_4 - (3 + \sqrt{5}) e_5 \right] = E_5$.

(vi) $a_1 = a_2 = a_3 = 0$, $a_4 = 1$ and $a_5 = 4\sqrt{5}$. Thus we have $E_5^1(z) = \left[ 2z + 2x - \zeta (e_1 + e_2 + e_3 + e_4) - (3 + 2\sqrt{5}) e_5, 2z - 2x - \zeta (e_1 + e_2 + e_3) - e_4 + (3\sqrt{5}) e_5, 2z - (e_1 + e_2) - \zeta e_4 - (3\sqrt{5} + 1) e_5, 2z - (e_2 + e_3) - \zeta e_4 - (3\sqrt{5} + 1) e_5, 2z - (e_1 + e_3) - \zeta e_4 - (3\sqrt{5} + 1) e_5 \right] = E_5$.

(vii) $a_1 = a_2 = 1$, $a_3 = a_4 = -1$ and $a_5 = 0$. Thus we have $E_5^1(z) = \left[ z + x + \zeta e_1 - \zeta e_2, z + x + \zeta e_2 - \zeta e_1, z - x + \zeta e_3 - \zeta e_4, z - x + \zeta e_4 - \zeta e_3, z \right] = E_5$.

(viii) $a_1 = a_2 = 2$, $a_3 = a_4 = -2$ and $a_5 = -5$. By Lemma 4 we have $E_5^1(z) = E_5^1$ by taking $u = 3x - \sqrt{5}(e_3 + e_4 + e_5)$.

(ix) $a_1 = 2$, $a_2 = 1$, $a_3 = -1$, $a_4 = -2$ and $a_5 = 2\sqrt{5}$. Then we have $E_5^1(z) = \left[ 2z + x - \sqrt{5} e_1 - \zeta e_2 - \zeta e_4 - 4 e_5, 2z - 2x - \zeta e_1 + \sqrt{5} e_3 + \sqrt{5} e_4 + (\zeta - 5) e_5, 2z + 2x - \sqrt{5} e_1 - \sqrt{5} e_2 - \zeta e_4 - (\zeta + 4) e_5, 2z - x - \zeta e_1 - \zeta e_3 + \sqrt{5} e_4 - 4 e_5, 2z - \sqrt{5} e_1 - \zeta e_2 - \zeta e_3 + \sqrt{5} e_4 - 4 e_5 \right] = E_5$.

Hence gen $E_5$ contains just two classes by Lemmas 7,8 and 9. \{E_5, E_j\} is a set of all representatives of classes in gen $E_5$. 

19
Proposition 12. Let $D = 13$. Then the class number of $E_n$ is one if $n \leq 2$, two if $n = 3$ and more than two if $n \geq 4$.

Proof. Let $n = 4$. Then there are three lattices $E_4$, $E_4(y_1)$ and $E_4(y_2)$ in gen $E_4$ with $\sqrt{13}y_1 = e_1 + 2e_2 + 3e_3 + 5e_4$ and $\sqrt{13}y_2 = e_1 + 2e_3 + 4e_4$. By Proposition 4 $Q(E_4(y_1)) \neq 1$, $Q(E_4(y_2)) \neq 1$ and $E_4(y_2) = E_4(y_1) \perp \mathbb{Z}$. Thus the class number of $E_4$ is more than 2. Let $n = 3$ and $\mathfrak{p} = (\sqrt{13})$. Take a $\mathfrak{p}$-adjacent lattice $E_3^1 = E_3(x)$ to $E_3$. By Lemma 5 and Proposition 4(5) we may consider $\sqrt{13}x = e_1 + 3e_2 + 4e_3$. Thus $Q(E_3^1) \neq 1$ and $E_3^1 = [x, y, z] = \left( \begin{array}{c} 2 \\ 0 \\ 1 \\ \sqrt{13} \\ 5 \end{array} \right)$, where $y = e_1 + e_2 - e_3$ and $z = 6x - \sqrt{13}(e_2 + 2e_3)$. Next consider a $\mathfrak{p}$-adjacent lattice $E_3^n = E_3^1(u)$ to $E_3^1$ with $\sqrt{13}u = ax + by + cz \in E_3^1 - \mathfrak{p}E_3^1$. If $\mathfrak{b} \in \mathfrak{p}$, then we may assume that $a = 0$ and $\alpha = 1$ by Lemma 2. Thus we may assume that $\gamma = 2$ or $\gamma = -5$ since $Q(u) \in \mathfrak{p}$ by Lemma 4. If $\gamma = 2$, then $E_3^n = [u, y, \sqrt{13}z] = [u, 4u + 2\gamma - \sqrt{13}z, 3u + 2y - \sqrt{13}z] = E_3$. If $\gamma = -5$, then $E_3^n = [u, y, \sqrt{13}z] = [u + 2y, 3u + y + \sqrt{13}z, 4u + 2y + \sqrt{13}z] = E_3$. Let $\mathfrak{b} \in \mathfrak{p}$. Then by Lemma 2 we may assume that $\alpha$ and $\beta$ are such that $|\alpha| \leq 6$ and $|\gamma| \leq 6$ and that $\beta = 2 \mod \sqrt{13}$. Since $\tau_x = \sqrt{13}y - 3z$, $\tau_{2x + 2\sqrt{13}y - 3z}$, $\tau_x \in 0(E_3^1)$, we may assume that $\sqrt{13}u = x + (\pm 2 + 2\sqrt{13})y - 6z$.

Hence $E_3^n = [u, \pm (5u - 9y) + x + (\pm 2\sqrt{13} - 2)z, 4u + 2x - 4y - (\pm 2 - \sqrt{13})z] = E_3$. By Lemmas 7, 8 and 9 we have the assertion.

Proposition 13. Let $D = 17$. Then the class number of $E_n$ is one if $n \leq 3$ and more than two if $n \geq 4$.

Proof. Let $n = 4$. Then there are three lattices $E_4$, $E_4(y_1)$ and $A$ in gen $E_4$, where $\sqrt{17}y_1 = e_1 + 3e_2 + 4e_3 + 5e_4$, $\sqrt{17}y_2 = e_1 + 2(e_2 + e_3 + e_4 + e_5)$ and $E_5(y_2) = \mathbb{Z} \perp A$. By Proposition 4 $Q(E_4(y_1)) \neq 1, 2$. By the Proposition 2 $Q(A) \neq 1$ and $Q(A) \neq 2$. Hence the class number of $E_4$ is more than two. Let $n = 3$. Then by Lemma 5 and the Proposition 4 a $(\sqrt{17})$-adjacent lattice to $E_3$ is isometric to $E_3$. 


Proposition 14. Let $D = 29$. Then the class number of $E_n$ is more than two if $n \geq 3$.

Proof. There are three lattices $E_3$, $E_3(y)$ and $E_3(y')$ in gen $E_3$, where $\sqrt{29}y = 2e_1 + 3e_2 + 4e_3$ and $2y' = e_1 + 1(1 + \sqrt{29})e_2 + 1(1 - \sqrt{29})e_3$. Then $E_3(y) = \{y\} \perp M$ with $1 \notin Q(M)$. Clearly $Q(E_3(y')) \neq 1$ since $E_3(y') = \{y', 2e_1, \sqrt{29}e_1 - 2e_2 + e_3\} = \left(\begin{array}{ccc} 1 & 4 & 0 \\ 2 & 29 & 31 \end{array}\right)$.

Proposition 15. Let $D = 33$. Then the class number of $E_n$ is one if $n \leq 2$, two if $n = 3$ and more than two if $n \geq 4$.

Proof. There are three lattices $E_4$, $E_4(x_1)$ and $E_4(x_2)$ in gen $E_4$ with $x_1 = \frac{\sqrt{33}}{11}(e_1 + e_2 + 3e_3)$ and $x_2 = \frac{\sqrt{33}}{11}(e_1 + e_2 + 2e_3 + 4e_4)$. Then $E_4(x_1) = E_3(x_1) \perp E_4$ with $1 \notin Q(E_3(x_1))$ and $1 \notin Q(E_4(x_2))$ by Proposition 4. Thus the class number of $E_4$ is more than two. Put $\pi = 11 + 2\sqrt{33}$ and $\omega = 6 + \sqrt{33}$. Let $n = 3$ and $\varphi = (\pi)$. Then a $\varphi$-adjacent lattice to $E_3$ is isometric to $E_3$ or $E_3(x_1)$ by Proposition 1 and Lemma 5. Note that $E_3(x_1) = \left\{e_1 - e_2, x_1 - e_1 - 2e_2 + e_3, 5x_1 + (1 - \sqrt{33})(e_1 + e_2), (3 - \sqrt{33})e_3\right\} \cong \left(\begin{array}{ccc} 2 & 1 & 0 \\ 1 & 3/3 & 3/3 \\ 0 & 3/3 & 3/3 \end{array}\right)$. Putting $x = \frac{\sqrt{33}}{3}(e_1 + e_2 + e_3)$, then $E_3 = E_3(x) = \left\{e_1 - e_2, x + (3 - \sqrt{33})e_1 + (1 - \sqrt{33})e_2 + e_3, x - 2(e_1 + e_2 + 4e_3)\right\} = E_3(x_1)$. To find a $\varphi$-adjacent lattice to $E_3(x_1)$ we have only to find a $\varphi$-adjacent lattice $E_3^\prime$ to $E_3$. Let $E_3^\prime = E_3^\prime(y)$ with $y \in \varphi^{-1}E_3 - E_3^\prime$. By Lemma 2 we can assume that $y = \frac{\sqrt{33}}{11}z$ with $z \in E_3 - \varphi E_3^\prime$. Thus $\varphi y \subset \omega E_3 \subset E_3$. Since $x \in E_3^\prime$ and $B(x, y) = B(e_1 + e_2 + e_3, z) \subset B(E_3^\prime, E_3^\prime) \subset 0$ we have $x + y \notin E_3^\prime$. For a vector $w \in E_3$ such that $B(w, x + y) \subset 0$ we have $\pi B(w, x) = B(w, \pi(x + y)) - B(w, \pi y) \subset 0$. Also $wB(w, x) \subset 0$. Hence $B(w, x) \subset 0$, so $w \in E_3^\prime$. And hence $B(w, y) = B(w, x + y) - B(w, x) \subset 0$, so $w \in E_3^\prime(y) = E_3^\prime$. Hence $E_3(x + y) \subset E_3^\prime$. Since
y = 2ω(x+y) - (2ωx+πy) with 2ωx+πy ∈ E₃ and B(y, 2ωx+πy) ∈ O, we have y ∈ E₃(x+y). For a vector w ∈ E₃ such that B(w,x) ∈ O and B(w,y) ∈ O, we have B(w,x+y) ∈ O. Thus E₃ ⊆ E₃(x+y). Hence E₃ = E₃(u)
with u = x+y = \frac{1}{\sqrt{33}}(11e₁+11e₂+11e₃+3z) ∈ \frac{1}{\sqrt{33}}E₃. Clearly \sqrt{33}u = \frac{3}{\sqrt{33}} \sum \alpha_i e_i with \alpha_i ∈ O. By Lemma 2 and considering the structure of O(E₃), we have only to consider the following three cases:

(i) \alpha₁ = \alpha₂ = 4 and \alpha₃ = 1. Then E₃ = \{u, 4u + 2(1-\sqrt{33})e₁ - 2(1+\sqrt{33})e₂, 4u - 4(1+\sqrt{33})e₁ + 4(1-\sqrt{33})e₂\} = E₃.

(ii) \alpha₁ = \alpha₂ = 2 and \alpha₃ = 5. Hence E₃ = \{u, 7u + 2(1-\sqrt{33})e₁ - 2(1+\sqrt{33})e₂, -\sqrt{33}e₃, 7u - 7(1+\sqrt{33})e₁ + 7(1-\sqrt{33})e₂ - \sqrt{33}e₃\} = E₃.

(iii) \alpha₁ = 1, \alpha₂ = 4 and \alpha₃ = 7. Thus E₃ = \{u, 4u - \sqrt{33}e₃, e₁ + 5e₂ - 3e₃\} = E₃.

Hence we have the assertion by Lemmas 7, 8 and 9.

Proposition 16. Let D = 41. Then the class number of Eₙ is

one if n = 1, two if n = 2, 3 and more than two if n ≥ 4.

Proof. By Proposition 6 there is a lattice G' in genE₂ such that 1 ∉ Q(G'). Hence there are three lattices E₄, G'⊥E₂ and G'⊥G' in genE₄. Thus the class number of E₄ is more than two.

Let n = 3 and \(\frac{D}{\sqrt{n}} = (\sqrt{4})\). A \(\frac{D}{\sqrt{n}}\)-adjacent lattice to E₃ is isometric to E₃ or E₃(x) with \(x = \frac{1}{\sqrt{4}}(e₁ + 2e₂ + 6e₃)\) by Propositions 1 and 4 and Lemma 3. Thus E₃ = E₃(x) = \{x, y, z\} = <1> · \begin{pmatrix} 5 & 2\sqrt{10} \\ 2\sqrt{10} & 5 \end{pmatrix} with y = 2e₁ - e₂ and z = \sqrt{4}t(e₁ + e₃) - 7x. Take a \(\frac{D}{\sqrt{n}}\)-adjacent lattice E₃ = E₃(u) to E₃ such that u ∉ E₃. Write \(\sqrt{4}u = \alpha x + \beta y + \gamma z\) with \(\alpha, \beta, \gamma \in O\). If \(\alpha \in \frac{D}{\sqrt{n}}\), then we may assume that \(\alpha = 0\) and \(\gamma = 20\) by Lemma 2. Since Q(u) ∉ O, we may assume that \(\beta = \pm 5 - 8\sqrt{10}\) by Lemma 2.
Thus \( E \frac{1}{3} = [x] \perp [-u, \pm 10u + (2\sqrt{4T} \pm 80)y - (8\pm 5\sqrt{4T})z] = E \frac{1}{3}. \) If \( \beta \in \mathcal{F}, \)
then we may assume that \( \alpha = 7, \beta = 0 \) and \( \gamma = 1. \) Hence \( u = e_1 + e_3 \) and 
\( E_3^1 = E_3. \) If \( \gamma \in \mathcal{F}, \) we may assume that \( \alpha = 6, \beta = 1 \) and \( \gamma = 0. \) Thus 
\( E_3^2 = [u] \perp [14u - 2\sqrt{4T}x - z] \perp [7u - \sqrt{4T}x - \sqrt{4T}y + 2z] = E_3. \) If \( \alpha \beta \gamma \notin \mathcal{F}, \)
then we may assume that \( \gamma = 1 \) and \( \beta \in Z \) by Lemma 2. Note that \( O(E_3^1) \)
contains the isometries \( "x + \pm x, y + 2\sqrt{4T}y - 5z, z + 33y - 2\sqrt{4T}z " \), \( "x + \pm x, \)
y + \( \frac{1}{2}(17-\sqrt{4T})y + \frac{1}{2}(3-\sqrt{4T})z, z + \frac{1}{2}(7\sqrt{4T} - 13)y - \frac{1}{2}(17-\sqrt{4T})z " \) and \( "x + \pm x, \)
y + \( \frac{1}{2}(17+\sqrt{4T})y - \frac{1}{2}(3+\sqrt{4T})z, y + \frac{1}{2}(13+7\sqrt{4T})y - \frac{1}{2}(17+\sqrt{4T})z " \). Hence by 
Lemmas 2 and 3 we have to consider the following two cases:

(i) \( \sqrt{4T}u = -(2\pm 3\sqrt{4T})x \pm 3y + z \) and (ii) \( \sqrt{4T}u = (10\pm 6\sqrt{4T})x \mp 30y + z. \) In 
the case of (i) we have \( E_3^2 = [u, \sqrt{4T}x, y \pm 13x] = [v] \perp [v_1, v_2] = E_3^1, \)
where 
\[
2v = (-19\sqrt{4T})u - (9\pm 3\sqrt{4T})\sqrt{4T}x + (5\pm \sqrt{4T})(y \mp 13x),
\]
\[
2v_1 = (11\pm \sqrt{4T})u + (15\pm 3\sqrt{4T})\sqrt{4T}x - (7\pm \sqrt{4T})(y \mp 13x)
\]
and 
\[
v_2 = 2(\pm 2\sqrt{4T})u + (\pm 19\pm 2\sqrt{4T})\sqrt{4T}x - (\pm 6\pm \sqrt{4T})(y \mp 13x).
\]
Then \( Q(v) = 1. \) In the case of (ii) we have \( E_3^2 = [u, \sqrt{4T}x, y \mp 15x] =
[v'] \perp [v_1', v_2'] = E_3^1, \)
where 
\[
2v' = (-9\pm \sqrt{4T})u - (-101\pm 11\sqrt{4T})\sqrt{4T}x - (-33\pm 7\sqrt{4T})(y \mp 15x),
\]
\[
v_1' = (21\pm \sqrt{4T})u - (236\pm 11\sqrt{4T})\sqrt{4T}x + (21\pm 15\sqrt{4T})(y \mp 15x)
\]
and 
\[
2v_2' = (25\pm 17\sqrt{4T})u - (273\pm 191\sqrt{4T})\sqrt{4T}x + (501\pm 11\sqrt{4T})(y \mp 15x).
\]
Then \( Q(v') = 1. \) Hence the class number of \( E_3 \) is two, and that of 
\( E_2 \) is also two, by Lemmas 7,8 and 9.
References


[9] H. Pfeuffer: On a conjecture about class numbers of totally positive quadratic forms in totally real algebraic number fields, J. Number Theory 11 (1979),


[11] R. Salamon: Die Klassen im Geschlecht von \( x_1^2+x_2^2+x_3^2 \) und \( x_1^2+x_2^2+x_3^2+x_4^2 \) über \( \mathbb{Z}[\sqrt{3}] \), Archiv Math. 20 (1969), 523-530.