OUKA
The University of Osaka
Institutional Knowledge Archive

Title	ON THE CLASS NUMBER OF A UNIT LATTICE OVER A RING OF REAL QUADRATIC INTEGERS
Author(s)	Mimura, Yoshio
Citation	大阪大学, 1983, 博士論文
Version Type	VoR
URL	https://hdl.handle.net/11094/27761
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

https://ir.library.osaka-u.ac.jp/

The University of Osaka

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

YOSHIO MIMURA

理 42
31
6250

§ 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 $n \geqq 3$, then the class number of E_n is one if and only if "$K = Q$, $n \leqq 8$", "$K = Q(\sqrt{2})$, $n \leqq 4$", "$K = Q(\sqrt{5})$, $n \leqq 4$", "$K = Q(\sqrt{17})$, $n = 3$", "$K = K^{(49)}$, $n = 3$" or "$K = K^{(148)}$, $n = 3$", where 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 $n \geqq 4$: If $n \geqq 4$, then the class number of E_n is two only if "$K = K^{(49)}$, $n = 4$" or "$K = Q(\sqrt{5})$, $n = 5,6,7$", 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 $K = Q(\sqrt{5})$ 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 ($\neq Q(\sqrt{2})$, $Q(\sqrt{5})$, $Q(\sqrt{17})$).

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 Q. Using this method Salamon ([11]) has found the first result for $Q(\sqrt{3})$. In this paper we shall prove the following theorem by using the Kneser method.

Theorem. In the case of real quadratic fields with $n \geqq 3$, the class number of E_n is two if and only if

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

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

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

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

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

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

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

$$A_p^n = \{(a_1,\ldots,a_n) \in Z^n \ ; \ \sum_{i=1}^{n} a_i^2 \equiv 0 \bmod p, \ (a_1,\ldots,a_n) \not\equiv (0,\ldots,0) \bmod p\}$$

where Z is the ring of rational integers. We define an equivalence relation $\sim$ on A_p^n : $(a_1,\ldots,a_n) \sim (b_1,\ldots,b_n)$ 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 $b_i^2 \equiv c\, a_{i'}^2 \bmod p$ for all i. In each equivalence class we can choose a representative $(a_1,\ldots,a_n)$ satisfying

$$0 \leqq a_1 \leqq a_2 \leqq \cdots \leqq a_n$$

and

$$\sum_{i=1}^{n} a_i^2 = \sum_{i=1}^{n} b_i^2 \text{ for all } (b_1,\ldots,b_n) \text{ in the class.}$$

By R_p^n we denote the set of the above representatives. Let $(a_1,\dots,a_n)$ and $(b_1,\dots,b_n)$ be in the same class and $(a_1,\dots,a_n) \in R_p^n$. We define the norm and the type of $(b_1,\dots,b_n)$ (or the class) :

$$N(b_1,\dots,b_n) = \frac{1}{p} \sum_{i=1}^{n} a_i^2 ,$$

$$T(b_1,\dots,b_n) = \min\{ \sum_{i=1}^{n} c_i^2 \ ; \ \sum_{i=1}^{n} c_i b_i \equiv 0 \bmod p, (c_1,\dots,c_n) \neq (0,\dots,0)\}.$$

It is easy to prove the following

Proposition 1. The number of the equivalence classes of the specified type T in A_p^3 is as follows :

	T = 1	T = 2	T = 3	$T \geqq 4$
p = 3	0	1	0	0
$p \equiv 1 \bmod 24$	1	1	1	(p-25)/24
$p \equiv 5 \bmod 24$	1	0	0	(p- 5)/24
$p \equiv 7 \bmod 24$	0	0	1	(p- 7)/24
$p \equiv 11 \bmod 24$	0	1	0	(p-11)/24
$p \equiv 13 \bmod 24$	1	0	1	(p-13)/24
$p \equiv 17 \bmod 24$	1	1	0	(p-17)/24
$p \equiv 19 \bmod 24$	0	1	1	(p-19)/24
$p \equiv 23 \bmod 24$	0	0	0	(p+ 1)/24

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

Let $K = Q(\sqrt{D})$ be a real quadratic field over Q with a square-free rational integer D and $\mathcal{O}$ be the ring of integers in K. By 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 $Q(L) \subset 2\mathcal{O}$. For vectors $x_1,\dots,x_m$ in V, $[x_1,\dots,x_m]$ denotes the lattice generated by $\{x_1,\dots,x_m\}$ over $\mathcal{O}$.

Let $\mathfrak{a}$ be a non-zero ideal of $\mathcal{O}$ and L be a unimodular lattice in V. For $x \in \mathfrak{a}^{-1}L$ such that $Q(x) \in \mathcal{O}$, we put

$$L(x) = \mathcal{O}x + \{z \in L \,;\, B(x,z) \in \mathcal{O}\},$$

which is called an $\mathfrak{a}$-adjacent lattice to L (Cf. [2]). The following Lemmas 1 - 4 are valid.

Lemma 1. Let L be a unimodular lattice and $L(x)$ be an $\mathfrak{a}$-adjacent lattice to L. Then $L(x)$ is unimodular. If $\mathfrak{a}$ is prime to $2\mathcal{O}$ or $L(x)_{\mathfrak{p}} \simeq L_{\mathfrak{p}}$ for any dyadic spot $\mathfrak{p}$, then an $\mathfrak{a}$-adjacent lattice to L belongs to gen L.

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

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

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

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 E_n is isometric to some $E_n(x)$ with $x = \frac{\sqrt{D}}{p}\sum_{i=1}^{n} a_i e_i$ and $(a_1,\ldots,a_n) \in R_p^n \cup \{(0,\ldots,0)\}$.

Proof. Note that $p\mathcal{O} = \mathfrak{p}^2$ and $\mathcal{O}/\mathfrak{p} \simeq Z/pZ$. Take an element $z = \sum_{i=1}^{n} \alpha_i e_i \in \mathfrak{p}^{-1} E_n$ with $Q(z) \in \mathcal{O}$. We can find $a_i \in Z$ such that

$$\sqrt{D}\,\alpha_i \equiv \frac{D}{p} a_i \mod \mathfrak{p}$$

since $\sqrt{D}\,\alpha_i \in \mathcal{O}$ and $\frac{D}{p}$ is prime to $\mathfrak{p}$. Put $x = \frac{\sqrt{D}}{p} \sum_{i=1}^{n} a_i e_i$. 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 $Q(z) \in \mathcal{O}$. Hence $Q(x) \in \mathcal{O}$ and $(a_1, \ldots, a_n) \in A_p^n$ if $x \notin E_n$. Since $-2B(x,z) = Q(z-x) - Q(x) - Q(z) \in \mathcal{O}$ and $B(x,z) \in \mathfrak{p}^{-2}$, we have $B(x,z) \in \mathcal{O}$. By Lemma 2 we have $E_n(z) = E_n(x)$. Considering the structure of $O(E_n)$, we may have $(a_1, \ldots, a_n) \in R_p^n \cup \{(0, \ldots, 0)\}$ 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 $n \geqq 3$. Consider the lattice $\bar{A} = E_n(z) = [z] \perp A$ with $z = \frac{1}{\sqrt{D}} \sum_{i=1}^{n} b_i e_i$. Then

1) $\bar{A} \in \operatorname{gen} E_n$,
2) A is even if $n \equiv b_1 \equiv \cdots \equiv b_n \equiv 1 \mod 2$,
3) $A \in \operatorname{gen} E_{n-1}$ unless $n \equiv b_1 \equiv \cdots \equiv b_n \equiv 1 \mod 2$,
4) $A \simeq E_2$ if $n = 3$, $D \equiv 1 \mod 4$ and $b_i = b_j$ for some $i < j$,
5) $1 \notin Q(A)$ 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 $\bar{A} \in \operatorname{gen} E_n$. 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 $B(v_i, v_j) \in Z$ and $\det(B(v_i, v_j)) = b_1^{2(n-2)} D \equiv 1 \mod 2$. The assertion (2) is clear. We shall show (3). Consider a lattice $M = [v_2, \ldots, v_n]$

over Z. Then $M_2 \simeq \langle 1\rangle \perp \cdots \perp \langle 1\rangle \perp \langle D\rangle$ or $M_2 \simeq \langle 1\rangle \perp \cdots \perp \langle 1\rangle \perp \langle D\rangle \perp \langle D\rangle \perp \langle D\rangle$ since M is not even and the Hasse symbol of M_2 takes the value +1, where M_2 is the $2Z$-completion of M. So $A_{\mathfrak{p}} \simeq E_{n-1\mathfrak{p}}$ since $O_{\mathfrak{p}} \supset Z_2$ 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 $\mathfrak{p}$ be dyadic. Then $A_{\mathfrak{p}} = [b_1 z - \sqrt{D}\, e_1, v_3, \ldots, v_n]_{\mathfrak{p}}$ with $\det(B(v_i, v_j)) = b_1^{2(n-3)}(D - b_2^2) \equiv 1 \bmod 4$. Thus $A_{\mathfrak{p}} \simeq [v_3, \ldots, v_n]_{\mathfrak{p}} \perp \langle D - b_2^2\rangle$. By a similar argument as in (i) we have $A_{\mathfrak{p}} \simeq E_{n-1\mathfrak{p}}$. By Lemma 1 we have $A \in \operatorname{gen} E_{n-1}$, and so $\overline{A} \in \operatorname{gen} E_n$.

(iii) Suppose that $n = 3$, $D \equiv 1 \bmod 4$ and $b_1 = b_2$. Thus $b_3 \equiv 1 \bmod 2$. Take f and g in Z such that $2b_2 f - b_3 g = 1$. Put

$$w_1 = -(b_3 f + b_2 g)z + f\sqrt{D}\, e_3 + \tfrac{1}{2}(1 + g\sqrt{D})\, e_1 + \tfrac{1}{2}(-1 + g\sqrt{D})\, e_2$$

and $w_2 = w_1 - e_1 + e_2$. Then $A = [w_1] \perp [w_2] \simeq E_2$.

(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 $a = \sum_{i=1}^{n} b_i d_i \in Z$, $\sum_{i=1}^{n} b_i c_i = 0$, $|a| \leqq \frac{1}{2}D$, $c_i \in \frac{1}{2}Z$, $d_i \in \frac{1}{2}Z$ and $c_i - d_i \in Z$ for all i. Thus

$$\begin{aligned} Q(u) &= \sum_{i=1}^{n} c_i^2 + D \sum_{i=1}^{n} d_i^2 - a^2 + 2\sqrt{D} \sum_{i=1}^{n} c_i d_i \\ &= \sum_{i=1}^{n} c_i^2 + \sum_{i<j} (b_i d_j - b_j d_i)^2 + 2\sqrt{D} \sum_{i=1}^{n} c_i d_i . \end{aligned}$$

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 $d_1/b_1 = \cdots = d_n/b_n = c$ for some $c \in Q$. 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 $D \equiv 1 \bmod 4$ 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 $c_i \in Z$ for all i and so $\sum_{i=1}^{n} c_i^2 \geqq 2$. 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 $\sum_{i<j}(b_id_j-b_jd_i)^2 \geqq n-1 \geqq 2$, so $Q(u) \neq 1$. Thus we may assume that $D \equiv 1 \bmod 4$ and $d_{i'} \notin Z$ for some i'. Thus $c_{i'} \notin Z$. Then $\sum_{i=1}^{n} c_i^2 \geqq \frac{1}{2}$ since $b_1b_2\cdots b_n \neq 0$. Hence

$$\sum_{i=1}^{n} c_i^2 + \sum_{i<j}(b_id_j-b_jd_i)^2 \geqq \frac{1}{2} + \frac{1}{4}(n-1) = \frac{1}{4}(n+1) \geqq 1$$

and the equality holds only when $n = 3$ and $\sum_{i=1}^{n} c_i^2 = \frac{1}{2}$. This case occurs only when $n = 3$ and $b_i = b_j$ for some $i < j$ since $\sum_{i=1}^{n} b_ic_i = 0$. 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 $D \neq 1,2,3,5,6,11,14,17,29,41$.

Proposition 3. Let $D \not\equiv 1 \bmod 4$. Let p be an odd prime dividing D. Consider the lattice $B = E_3(y)$ with $y = \frac{\sqrt{D}}{p}\sum_{i=1}^{3} a_ie_i$ and $(a_1,a_2,a_3) \in R_p^3$. Then

(1) $B \in \mathrm{gen}\, E_3$,

(2) $B \simeq E_1 \perp B'$ and $1 \notin Q(B')$ if $D = p = \sum_{i=1}^{3} a_i^2$ or if $T(a_1,a_2,a_3) = 1$,

(3) $1 \notin Q(B)$ if $T(a_1,a_2,a_3) \geqq 2$ and unless $D = p = \sum_{i=1}^{3} a_i^2$.

Proof. By Lemma 1 we have $B \in \mathrm{gen}\, E_3$. Suppose that $T(a_1,a_2,a_3) \geqq 2$ 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 $a \in Z$, $c_i \in Z$, $d_i \in Z$, $\sum_{i=1}^{3} a_ic_i \equiv 0 \bmod p$ and $|a| < \frac{1}{2}p$.

Then

$$1 = Q(u) = \sum_{i=1}^{3} c_i^2 + \frac{D}{p}\frac{1}{p} \sum_{i=1}^{3} (aa_i+pd_i)^2 + \frac{2\sqrt{D}}{p} \sum_{i=1}^{3} c_i(aa_i+pd_i).$$

Hence we have $\sum_{i=1}^{3} c_i^2 = 0$ and $D = p = \sum_{i=1}^{3} (aa_i+pd_i)^2$ since $T(a_1,a_2,a_3) \geqq 2$. Thus the assertion (3) holds. Now let $D = p = \sum_{i=1}^{3} a_i^2$. Then $B = [y] \perp B'$ and $Q(B') \not\ni 1$ 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 $D \equiv 1 \bmod 4$ 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 $(a_1,\ldots,a_n) \in R_p^n$. Assume that $n \geqq 3$. 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) $B \simeq E_1 \perp B'$ 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 $T \geqq 3$,

(5) $B \simeq E_3$ if $n = 3$, $D = p$ and $T \leqq 2$,

(6) $B \simeq E_1 \perp B'$ with $1 \notin Q(B')$ if $D = p$, $N = 1$ and $T \geqq 3$,

(7) $1 \notin Q(B)$ if $D = p$, $N = 2$ and $T \geqq 3$,

(8) $1 \notin Q(B)$ if $D = p$, $N \geqq 3$ and $T \geqq 2$,

(9) $2 \notin Q(B)$ if $n = 3$, $D = p$, $N \geqq 3$ and $T \geqq 3$,

(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 $a \in Z$, $|a| < \frac{1}{2}p$, $c_i \in \frac{1}{2}Z$, $d_i \in \frac{1}{2}Z$, $c_i - d_i \in Z$ and $2\sum_{i=1}^{n} a_i c_i \equiv 0 \bmod p$. Then

$$Q(u) = X + Y + \frac{2\sqrt{D}}{p} \sum_{i=1}^{n} c_i(aa_i+pd_i),$$

where $X = \sum_{i=1}^{n} c_i^2$ and $Y = \frac{D}{p}\frac{1}{p}\sum_{i=1}^{n} (aa_i+pd_i)^2$. If $Y = 0$, then $a = d_i = 0$ for all i, so $c_i \in Z$ for all i. Thus $X \geqq T$. If $X = 0$ and $Y \neq 0$, then $c_i = 0$ for all i and $Y \geqq DN/p$. If $X \neq 0$ and $Y \neq 0$, then $X + Y \geqq \frac{T}{4} + \frac{D}{p}\frac{N}{4}$. Thus (3),(7),(8) and the half of (4) hold. Now suppose that $D \neq p$ and $T \geqq 3$ or that $D = p$, $T \geqq 3$, $N \geqq 3$ and $n = 3$. Thus $X \geqq 3/4$ and $Y \geqq 3/4$. If $X = 3/4$ with $Y = 5/4$ or $X = 5/4$ with $Y = 3/4$, then we have $2 \equiv 4X - 4Y \equiv \sum_{i=1}^{n} (2c_i)^2 - \sum_{i=1}^{n} (2d_i)^2 \equiv 0 \bmod 4$, which is a contradiction. If $X = Y = 1$, then $D = p$ and $\sum_{i=1}^{n} c_i^2 = 1$. Thus $D = p$ and $n \geqq 4$, which is a contradiction. Hence (9) and the rest of (4) hold. If $n = 3, D \neq p$ and $T = 1$, then $a_1 = 0$ 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 $T \leqq 2$. Then $N = 1$. If $T = 1$, then $B = [e_1] \perp [y] \perp [y'] \simeq E_3$ with $y' = \frac{1}{\sqrt{p}}(a_3e_2 - a_2e_3)$. If $T = 2$, then $B \simeq E_3$ by Proposition 2,(4). Thus (5) holds. Finally (6) follows from Proposition 2,(5).

Proposition 5. Let $D \equiv 3 \bmod 4$. Consider the lattice $C = E_3(x) = [e_3] \perp C'$ with $x = \frac{1}{2}(e_1 + \sqrt{D}\, e_2)$. Then

(1) $C \in \operatorname{gen} E_3$,

(2) $1 \notin Q(C')$ if $D > 3$,

(3) C' is even if and only if $D \equiv 7 \bmod 8$.

Proof. We have $C' = [x, 2e_2] \simeq \begin{pmatrix} \frac{1}{4}(D+1) & \sqrt{D} \\ \sqrt{D} & 4 \end{pmatrix}$. Let $\mathfrak{p}$ be dyadic. If $D \equiv 3 \bmod 8$, then C' is not even and $C'_{\mathfrak{p}} \simeq \langle \frac{1}{4}(D+1)\rangle \perp \langle \frac{1}{4}(D+1)\rangle \simeq E_{2\mathfrak{p}}$ since $3 \in K_{\mathfrak{p}}^2$. If $D \equiv 7 \bmod 8$, then C' is even and $C'_{\mathfrak{p}} \simeq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, so $C_{\mathfrak{p}} \simeq \langle 1\rangle \perp \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \simeq E_{3\mathfrak{p}}$ since $-1 \in K_{\mathfrak{p}}^2$. Thus (1) and (3) are proved by Lemma 1. It is easy to show (2) directly.

Proposition 6. Let $D \equiv 5 \bmod 12$. Consider the lattice $G = E_3(x) = [e_3] \perp G'$ with $x = \frac{1}{3}(e_1 + D\sqrt{D}\, e_2)$. Then

(1) $G \in \operatorname{gen} E_3$ and $G' \in \operatorname{gen} E_2$,

(2) $1 \notin Q(G')$ and $2 \notin Q(G')$ if $D \geqq 29$.

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 $p \equiv 1 \bmod 12$. Then the number of the classes in A_p^3 whose type is six is one or zero according as $p \equiv 1 \bmod 24$ or $p \equiv 13 \bmod 24$. Let $(a_1, a_2, a_3) \in R_p^3$ with $T = T(a_1, a_2, a_3) \geqq 3$ 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 $(b_1, b_2, b_3) \in A_p^3$ whose type is six. Thus we may assume that $b_3 = 2b_1 + b_2$. Hence $0 \equiv \sum_{i=1}^{3} b_i^2 \equiv 2(b_1+b_2)^2 + 3b_1^2 \bmod p$. So $(\frac{-6}{p}) = 1$, i.e., $p \equiv 1 \bmod 24$. If $p \equiv 1 \bmod 24$, then there is an integer c such that $c^2 \equiv -6 \bmod p$. Hence $\pm c(b_1+b_2) \equiv 3b_1 \bmod p$. 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 $T \geqq 7$. 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 $a \in \mathbb{Z}$, $|a| < \frac{1}{2}p$, $c_i \in \frac{1}{2}\mathbb{Z}$, $d_i \in \frac{1}{2}\mathbb{Z}$, $c_i - d_i \in \mathbb{Z}$, $2\sum_{i=1}^{3} a_ic_i \equiv 0 \bmod p$.

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 $Y =$

$\frac{1}{p}\sum_{i=1}^{3}(a\,a_i + p\,d_i)^2$. 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 $1 \equiv \sum_{i=1}^{3}(2c_i)^2 \equiv \sum_{i=1}^{3}(2d_i)^2 \equiv \sum_{i=1}^{3}(2aa_i+2pd_i)^2 = 3p \equiv 3 \bmod 4$. This is a contradiction. In the case (iii) we have $(a_1, a_2, a_3) \sim (c, 3-c, 3+c)$ for an integer c with $c^2+6 \equiv 0 \bmod p$ by the argument used above since $X = 6/4$. Since T must be five we have $c \equiv \pm1, \pm2, \pm3, \pm6$ or $\pm9 \bmod p$, which is a contradiction to the fact that p divides c^2+6. In the case (i) we have $c_i = 0$ and $d_i \in Z$ for all i. Hence we can write $u_1 = ax + \sqrt{p}\sum_{i=1}^{3} d_i e_i = \frac{1}{\sqrt{p}}\sum_{i=1}^{3} f_i e_i$ 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 $a, a', d_i, d_i', f_i, f_i' \in Z$. Thus $f_i \equiv a\,a_i \bmod p$ and $f_i' \equiv a'\,a_i \bmod p$. Hence $f_i f_j' - f_j f_i' \equiv 0 \bmod p$. Since $3p^2 = (2p)^2 - p^2 = \sum_{i=1}^{3} f_i^2 \sum_{i=1}^{3} f_i'^2 - (\sum_{i=1}^{3} f_i f_i')^2 = \sum_{i<j}(f_i f_j' - f_j f_i')^2$, we have $f_i f_j' - f_j f_i' = h_{ij}\,p = \pm p$ 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., $a_1 h_{23} + a_2 h_{31} + a_3 h_{12} \equiv 0 \bmod p$. This implies that $T \leqq 3$. This is a contradiction.

Proposition 8. Let $n \geqq 3$. 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 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 $(a_1, a_2, a_3) \in R_q^3$ 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 $(a_1, a_2, a_3) \in R_p^3$ 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 $M \simeq E_1 \perp M'$ with $1 \notin Q(M')$.

(ii) Let $D \equiv 3 \mod 8$. For L we take a lattice $\overline{A} \simeq E_1 \perp A$ with an even lattice A in the Proposition 2. For M we take the lattice $C \simeq E_1 \perp C'$ 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 $C \simeq E_1 \perp C'$ 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 $(a_1, a_2, a_3) \in R_p^3$ and $(a_1', a_2', a_3') \in R_q^3$ for some prime divisors p and q of D (possibly $p = q$) such that $T(a_1, a_2, a_3) = 1$ and $T(a_1', a_2', a_3') \geqq 2$ or such that $T(a_1, a_2, a_3) = 2$ and $T(a_1', a_2', a_3') \geqq 3$. 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 $(a_1, a_2, a_3) \in R_p^3$ whose type is more than two, for which we can consider the lattice B with $Q(B) \not\ni 1$ in ~~the~~ Proposition 4. Put

$L = B$. There are positive integers b_1, b_2 and b_3 such that $b_1^2 + b_2^2 + b_3^2 = D$ since $D \equiv 1 \bmod 4$ and $p \equiv 3 \bmod 4$. We have $b_i \neq b_j$ whenever $i \neq j$ since $(\frac{-2}{p}) = -1$. Hence we can consider a lattice $\overline{A} = E_1 \perp A$ with $1 \notin Q(A)$. Put $M = \overline{A}$.

(v) Let D be a prime $p \equiv 1 \bmod 12$. Since $p = 3a^2 + b^2$ for some positive integers a and b, we can consider the lattice A for (a,a,a,b) in the Proposition 2. Put $L = A$. 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 $p \equiv 1 \bmod 24$. Then there are at least two elements (a_1, a_2, a_3) and (a_1', a_2', a_3') in 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 $M = B$ for (a_1, a_2, a_3) in Proposition 4. Hence $M \neq E_3$. And $M \neq L$ if $N(a_1, a_2, a_3) \neq 2$. If $M \simeq L$ 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 $p \equiv 13 \bmod 24$. There is an element $(a_1, a_2, a_3) \in R_p^3$ whose type is more than three by ~~the~~ Proposition 1. For M we take the lattice B for (a_1, a_2, a_3) in ~~the~~ Proposition 4. If $N(a_1, a_2, a_3) = 1$, then $B = E_1 \perp B'$ 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 $B \neq L$ by ~~the~~ Proposition 7.

(vi) Let D be a prime $p \equiv 5 \bmod 12$. For L we take the lattice A with $1 \notin Q(A)$ in ~~the~~ Proposition 2. For M we take the lattice $G = E_1 \perp G'$ with $1 \notin Q(G')$ in ~~the~~ 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 $V = K E_n$ and $P = \theta(O^+(V))$, where θ 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 ~~the~~ Theorem 104:9 in [4]:

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

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

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

Lemma 9. Let $n \geqq 3$, $\mathfrak{p}$ be a spot dividing D and $M \in \text{gen}\, E_n$ with $M_{\mathfrak{q}} = E_{n\mathfrak{q}}$ 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

$$E_n = L_0, \ L_1, \dots, \ L_t = M$$

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 $E_{n\mathfrak{p}} = L_0^{(\mathfrak{p})}$, $L_1^{(\mathfrak{p})}, \dots, L_t^{(\mathfrak{p})} = M_{\mathfrak{p}}$ in $V_{\mathfrak{p}}$ with $L_{i+1}^{(\mathfrak{p})}$ $\mathfrak{p}$-adjacent to $L_i^{(\mathfrak{p})}$ and $L_i^{(\mathfrak{p})} \cong E_{n\mathfrak{p}}$. Put $L_0 = E_n$. Then $M_{\mathfrak{p}} = \sigma L_{0\mathfrak{p}}$ for some $\sigma \in O(V_{\mathfrak{p}})$. By expressing σ as a product of symmetries on $V_{\mathfrak{p}}$ we see that it is enough if we assume that σ is a symmetry. Then $\sigma = \tau_u$ with u a maximal anisotropic vector in $L_{0\mathfrak{p}}$. Then there is either a 1- or 2-dimensional unimodular sublattice K of $L_{0\mathfrak{p}}$ which contains u. If the rank of K is one, then $L_{0\mathfrak{p}} = \tau_u L_{0\mathfrak{p}} = M_{\mathfrak{p}}$, so $M_{\mathfrak{p}}$ is $\mathfrak{p}$-adjacent to $L_{0\mathfrak{p}}$. If the rank of K is two, then we take the splitting $L_{0\mathfrak{p}} = K \perp K'$. Then $K' = \tau_u K' \subset M_{\mathfrak{p}}$ and so we have a splitting $M_{\mathfrak{p}} = K'' \perp K'$. Write $K = \mathfrak{p}^r x + \mathcal{O}_{\mathfrak{p}} y$ and $K'' = \mathcal{O}_{\mathfrak{p}} x + \mathfrak{p}^r y$ with a non-negative integer r. Hence we may put $L_0^{(\mathfrak{p})} = L_{0\mathfrak{p}}$, $L_1^{(\mathfrak{p})} = (\mathfrak{p}^{r-1} x + \mathfrak{p} y) \perp K' = L_0^{(\mathfrak{p})}(\pi^{r-1}x)$, $\ldots$, $L_r^{(\mathfrak{p})} = M_{\mathfrak{p}} = K'' \perp K' = (\mathcal{O}_{\mathfrak{p}} x + \mathfrak{p}^r y) \perp K' = L_{r-1}^{(\mathfrak{p})}(x)$, where $\mathfrak{p} = \pi \mathcal{O}_{\mathfrak{p}}$. We must show that $L_i^{(\mathfrak{p})} \simeq E_{n\mathfrak{p}}$. It is trivial when $i = 0$ or $i = r$. Assume that $1 \leq i \leq r-1$. If $\mathfrak{p}$ is non-dyadic, then $\mathfrak{p}^{r-i} x + \mathfrak{p}^i y \simeq \langle 1 \rangle \perp \langle -1 \rangle \simeq K$, so $L_i^{(\mathfrak{p})} \simeq K \perp K' \simeq E_{n\mathfrak{p}}$. If $\mathfrak{p}$ is dyadic, then n is odd, hence $K' = [z] \perp K'''$ with $Q(z) = \varepsilon$ a unit in $\mathcal{O}_{\mathfrak{p}}$. It is enough to show that $(\mathfrak{p}^r x + \mathcal{O}_{\mathfrak{p}} y) \perp \mathcal{O}_{\mathfrak{p}} z \simeq (\mathfrak{p}^{r-i} x + \mathfrak{p}^i y) \perp \mathcal{O}_{\mathfrak{p}} z$ for $1 \leq i \leq r-1$. We can assume that $\mathfrak{p}^r B(x,y) = \mathcal{O}_{\mathfrak{p}}$. Since $y \in K \subset L_{0\mathfrak{p}} \simeq E_{n\mathfrak{p}}$ and $\mathfrak{p} = \sqrt{2}\mathcal{O}_{\mathfrak{p}}$, we have $Q(y) \equiv 0$ or $1 \bmod 2$. Similarly $Q(x) \equiv 0$ or $1 \bmod 2$ and $\varepsilon \equiv 1 \bmod 2$. If $Q(y) \equiv 0 \bmod 2$, then $(\mathfrak{p}^r x + \mathcal{O}_{\mathfrak{p}} y) \perp \mathcal{O}_{\mathfrak{p}} z \simeq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \perp \langle \varepsilon \rangle \simeq (\mathfrak{p}^{r-i} x + \mathfrak{p}^i y) \perp \mathcal{O}_{\mathfrak{p}} z$. If $Q(y) \equiv 1 \bmod 2$ and $\pi^{2r} Q(x) \equiv 0 \bmod 8$, then $(\mathfrak{p}^r x + \mathcal{O}_{\mathfrak{p}} y) \perp \mathcal{O}_{\mathfrak{p}} z \simeq \langle Q(y) \rangle \perp \langle -Q(y) \rangle \perp \langle \varepsilon \rangle \simeq \langle \varepsilon \rangle \perp \langle -\varepsilon \rangle \perp \langle \varepsilon \rangle \simeq \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \perp \langle \varepsilon \rangle \simeq (\mathfrak{p}^{r-i} x + \mathfrak{p}^i y) \perp \mathcal{O}_{\mathfrak{p}} z$. If $Q(x) \equiv Q(y) \equiv 1 \bmod 2$, $r=2$ and $i=1$, then $(\mathfrak{p}^2 x + \mathcal{O}_{\mathfrak{p}} y) \perp \mathcal{O}_{\mathfrak{p}} z \simeq \langle Q(y) \rangle \perp \langle 3Q(y) \rangle \perp \langle \varepsilon \rangle \simeq \langle \varepsilon \rangle \perp \langle 3\varepsilon \rangle \perp \langle \varepsilon \rangle \simeq \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix} \perp \langle \varepsilon \rangle \simeq (\mathfrak{p} x + \mathfrak{p} y) \perp \mathcal{O}_{\mathfrak{p}} z$.

Proposition 9. Let $D = 2$. 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. There are three lattices E_6, $E_6(\frac{1}{\sqrt{2}}(e_1+\cdots+e_4))$ and $E_6(\frac{1}{\sqrt{2}}(e_1+\cdots+e_6))$ in $\mathrm{gen}\,E_6$, any two of which are not isometric. Let $n=5$. Take $\mathfrak{p}=(\sqrt{2})$ and a $\mathfrak{p}$-adjacent lattice $E_5(x)$ in $\mathrm{gen}\,E_5$. Write $x=\frac{1}{\sqrt{2}}\sum_{i=1}^{5}\alpha_i e_i$. Note that $O(E_5)$ contains all permutations of $\{e_1,\ldots,e_5\}$. And note that $Q(x)\equiv 0$ or $1 \bmod 2$ since $E_5(x)\in \mathrm{gen}\,E_5$. By Lemmas 2 and 3 we have only to consider the following three cases: (i) $\alpha_1=\alpha_2=\alpha_3=\alpha_4=\alpha_5=0$. Then $E_5(x) = E_5$. (ii) $\alpha_1=\alpha_2=1$ and $\alpha_3=\alpha_4=\alpha_5=0$. Then $E_5(x)\simeq E_5$. (iii) $\alpha_1=\alpha_2=\alpha_3=\alpha_4=1$ and $\alpha_5=0$. Then $E_5(x)=E_4^0\perp[e_5]$, where $E_4^0=E_4(u)$ with $u=\frac{1}{\sqrt{2}}(e_1+\cdots+e_4)$. Hence a $\mathfrak{p}$-adjacent lattice to E_5 in $\mathrm{gen}\,E_5$ is isometric to E_5 or $E_5^!=E_4^0\perp[e_5]$. Next take a $\mathfrak{p}$-adjacent lattice $E_5^!(y)$ to $E_5^!$ in $\mathrm{gen}\,E_5$ and write $\sqrt{2}\,y=w+\alpha e_5$ with $\alpha\in\mathcal{O}$ and $w\in E_4^0$. Since $Q(y)\in\mathcal{O}$ and E_4^0 is even, we have $\alpha\in\mathfrak{p}$. By Lemma 2 we have $E_5^!(y)=E_5^!(\frac{1}{\sqrt{2}}w)=E_4^0(\frac{1}{\sqrt{2}}w)\perp[e_5]$. Hence we may write $\sqrt{2}\,y=au+\sum_{i=1}^{4}\alpha_i e_i$ where $\alpha_i\in\mathcal{O}$, $a\in\{0,1\}$ and $\sum_{i=1}^{4}\alpha_i\equiv 0 \bmod \sqrt{2}$. Note that $Q(y)\equiv 0$ or $1 \bmod 2$ since $E_5^!(y)\in \mathrm{gen}\,E_5$. If $a=0$, then we have the following four cases by Lemmas 2 and 3: (i) $\alpha_1=\alpha_2=\alpha_3=\alpha_4=0$. Then $E_5^!(y)=E_5^!$. (ii) $\alpha_1=\sqrt{2}$ and $\alpha_2=\alpha_3=\alpha_4=0$. Then $E_5^!(y)=E_5$. (iii) $\alpha_1=\alpha_2=1$ and $\alpha_3=\alpha_4=0$. Then $E_5^!(y)=E_4^0(y)\perp[e_5]=E_2(\frac{1}{\sqrt{2}}(e_1+e_2))\perp E_2(\frac{1}{\sqrt{2}}(e_3+e_4))\perp[e_5]\simeq E_5$. (iv) $\alpha_1=\alpha_2=1$, $\alpha_3=\sqrt{2}$ and $\alpha_4=0$. Then $E_5^!(y)\simeq E_5^!$. Next consider the case of $a=1$. Since $\tau_{e_1}\in O(E_5^!)$, we have $\sqrt{2}\,y\tau_{e_1}= u+(-\alpha_1-\sqrt{2})e_1+\alpha_2e_2+\cdots$. Hence we may assume that $\alpha_i\equiv 0 \bmod 2$ or $\alpha_i\equiv 1 \bmod 2$. Thus we have only to consider the following cases by Lemmas 2 and 3: (v) $\alpha_1=\alpha_2=\alpha_3=\alpha_4=0$ or $\alpha_1=\alpha_2=\alpha_3=\alpha_4=1$. Then $E_5^!(y)\simeq E_5$. (vi) $\alpha_1=-1$, $\alpha_2=1$ and $\alpha_3=\alpha_4=0$. Apply Lemma 4 to this case taking $w=u-\sqrt{2}\,e_1$. Then $E_5^!(y)\simeq E_4^0\perp[e_5]$

$\simeq E_5^!$. Thus a $\mathfrak{p}$-adjacent lattice to $E_5^!$ is isometric to E_5 or $E_5^!$. Hence $\{E_5^!, E_5\}$ is a set of all representatives of classes in $\mathrm{gen}\, E_5$ by Lemmas 7,8 and 9. By ~~the~~ Theorem 105:1 in [4] this implies that the class number is one if $n \leqq 4$.

From [11] we have

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

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

Proof. Put $x = \frac{1}{\sqrt{5}}(e_1 + \cdots + e_5)$, $y_1 = \frac{1}{\sqrt{5}}(e_1 + e_2 + 2e_3 + 2e_4)$ and $x_1 = \frac{1}{\sqrt{5}}(e_1 + e_2 + e_3 + 2e_4 + 2e_5 + 2e_6)$. Consider the lattice $E_5^! = E_5(x) = [x] \perp E_4^o$. Then E_4^o is even. If $n = 6$, then we have three lattices E_6, $E_6(x)$ and $E_6^! = E_6(x_1)$ in $\mathrm{gen}\, E_6$. By Proposition 4,(8) we have $1 \notin Q(E_6^!)$. Thus the class number of E_6 is more than two. Let $\mathfrak{p} = (\sqrt{5})$ and $n = 5$. Take a $\mathfrak{p}$-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 $(a_1, \ldots, a_5) \in R_5^5$. Hence $y \in \{0, x, \frac{1}{\sqrt{5}}(e_1 + 2e_2), y_1\}$. Thus $E_5(0) = E_5$, $E_5(x) = E_5^!$ and $E_5(\frac{1}{\sqrt{5}}(e_1 + 2e_2)) \simeq E_5$. By the Lemma 4 $E_5(y_1) \simeq E_5$ taking $w = \frac{1}{2}(1+\sqrt{5})(e_3 + e_4) \in E_5$. Take a $\mathfrak{p}$-adjacent lattice $E_5^!(z)$ to $E_5^!$. By Lemma 2 we may assume that $\sqrt{5}\, z = a x + \sum_{i=1}^{5} \alpha_i e_i$ where $a = 0$ or 1, $\alpha_i = a_i + b_i\sqrt{5} \in Z[\sqrt{5}]$ and $\sum_{i=1}^{5} a_i \equiv 0 \bmod 5$. 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 $E_5^!(z) = E_5^!$ or $E_5^!(z) = E_5$ according as $\sum_{i=1}^{5} b_i \equiv 0 \bmod 5$ or not.

(ii) $a_1 = \cdots = a_5 = 1$. Thus $z = x + \sum_{i=1}^{5} b_i e_i$ with $\sum_{i=1}^{5} b_i \equiv 0 \bmod 5$, so $z \in E_5^!$. Hence $E_5^!(z) = E_5^!$.

(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 $z \in E_5^!$, so $E_5^!(z) = E_5^!$. If $b_5 = 1$, then we have $E_5^!(z) = [z_0, z_1, \ldots, z_4] \simeq E_5$, where $z_0 = z + \bar\zeta e_3 + \zeta e_4 - e_5$, $z_1 = z + x + \bar\zeta e_1 + \bar\zeta e_3 - e_5$, $z_2 = z + 2x + \bar\zeta e_1 - \sqrt{5}e_3 - \zeta e_5$, $z_3 = z - 2x + \zeta e_2 + \sqrt{5}e_4 - \bar\zeta e_5$ and $z_4 = z - x + \zeta e_2 + \zeta e_4 - e_5$, where $\zeta = \frac{1}{2}(1+\sqrt{5})$.

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

(iv) $\alpha_1 = \cdots = \alpha_4 = 0$ and $\alpha_5 = 2\sqrt{5}$. Thus $E_5^!(z) = [2z - 5e_5,\ 2z - e_1 - 4e_5,\ 2z - e_2 - 4e_5,\ 2z - e_3 - 4e_5,\ 2z - e_4 - 4e_5] \simeq E_5$.

(v) $\alpha_1 = \alpha_2 = \alpha_3 = 0$, $\alpha_4 = 2$ and $\alpha_5 = 3 + 3\sqrt{5}$. Thus $E_5^!(z) = [z + 2x - \zeta e_4 - (3+\sqrt{5})e_5,\ z - 2x - \bar\zeta(e_1 + e_2 + e_3) - (3+\zeta)e_5,\ z - e_1 - \zeta e_4 - (3+\zeta)e_5,\ z - e_2 - \zeta e_4 - (3+\zeta)e_5,\ z - e_3 - \zeta e_4 - (3+\zeta)e_5] \simeq E_5$.

(vi) $\alpha_1 = \alpha_2 = \alpha_3 = 0$, $\alpha_4 = 1$ and $\alpha_5 = 4+\sqrt{5}$. Thus we have $E_5^!(z) = [2z + 2x - \zeta(e_1+e_2+e_3+e_4) - (3+2\sqrt{5})e_5,\ 2z - 2x - \bar\zeta(e_1+e_2+e_3) - e_4 + (3\zeta-4)e_5,\ 2z - (e_1+e_2) - \zeta e_4 - (3\zeta+1)e_5,\ 2z - (e_2+e_3) - \zeta e_4 - (3\zeta+1)e_5,\ 2z - (e_1+e_3) - \zeta e_4 - (3\zeta+1)e_5] \simeq E_5$.

(vii) $\alpha_1 = \alpha_2 = 1$, $\alpha_3 = \alpha_4 = -1$ and $\alpha_5 = 0$. Thus we have $E_5^!(z) = [z + x + \bar\zeta e_1 - \zeta e_2,\ z + x + \bar\zeta e_2 - \zeta e_1,\ z - x + \zeta e_3 - \bar\zeta e_4,\ z - x + \zeta e_4 - \bar\zeta e_3, z] \simeq E_5$.

(viii) $\alpha_1 = \alpha_2 = 2$, $\alpha_3 = \alpha_4 = -2$ and $\alpha_5 = -5$. By Lemma 4 we have $E_5^!(z) \simeq E_5^!$ by taking $\omega = 3x - \sqrt{5}(e_3 + e_4 + e_5)$.

(ix) $\alpha_1 = 2$, $\alpha_2 = 1$, $\alpha_3 = -1$, $\alpha_4 = -2$ and $\alpha_5 = 2\sqrt{5}$. Then we have $E_5^!(z) = [2z + x - \sqrt{5}e_1 - \zeta e_2 - \bar\zeta e_4 - 4e_5,\ 2z - 2x - \zeta e_1 + \sqrt{5}e_3 + \sqrt{5}e_4 +$ ([illegible]$\zeta - 5)e_5,\ 2z + 2x - \sqrt{5}e_1 - \sqrt{5}e_2 - \bar\zeta e_4 - (\zeta+4)e_5,\ 2z - x - \zeta e_1 - \bar\zeta e_3 + \sqrt{5}e_4 - 4e_5,\ 2z - \sqrt{5}e_1 - \zeta e_2 - \bar\zeta e_3 + \sqrt{5}e_4 - 4e_5] \simeq E_5$.

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

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

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 $\sqrt{13}y_2 = e_1+3e_2+4e_3$. By the Proposition 4 $Q(E_4(y_1)) \not\ni 1$, $Q(E_3(y_2)) \not\ni 1$ and $E_4(y_2) = E_3(y_2) \perp [e_4]$. 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 $E_3' = E_3(x)$ to E_3. By Lemma 5 and the Proposition 4(5) we may consider $\sqrt{13}x = e_1+3e_2+4e_3$. Thus $Q(E_3') \not\ni 1$ and $E_3' = [x, y, z] \simeq \begin{pmatrix} 2 & 0 & 1 \\ 0 & 3 & \sqrt{13} \\ 1 & \sqrt{13} & 5 \end{pmatrix}$, where $y = e_1+e_2-e_3$ and $z = 6x - \sqrt{13}(e_2+2e_3)$. Next consider a $\mathfrak{p}$-adjacent lattice $E_3'' = E_3'(u)$ to E_3' with $\sqrt{13}u = \alpha x+\beta y+\gamma z \in E_3' - \mathfrak{p}E_3'$. If $\beta \in \mathfrak{p}$, then we may assume that $\beta = 0$ and $\alpha = 1$ by Lemma 2. Thus we may assume that $\gamma = 2$ or $\gamma = -5$ since $Q(u) \in \mathcal{O}$ by Lemma 4. If $\gamma = 2$, then $E_3'' = [u, y, \sqrt{13}z] = [u-y, 4u+2y-\sqrt{13}z, 3u+2y-\sqrt{13}z] \simeq E_3$. If $\gamma = -5$, then $E_3'' = [u, y, \sqrt{13}z] = [u+2y, 3u+y+\sqrt{13}z, 4u+2y+\sqrt{13}z] \simeq E_3$. Let $\beta \notin \mathfrak{p}$. Then by Lemma 2 we may assume that α and $\beta \in Z$ such that $|\alpha| \leqq 6$ and $|\gamma| \leqq 6$ and that $\beta \equiv 2 \bmod \sqrt{13}$. Since $\tau_{x+\sqrt{13}y-3z}$, $\tau_{2x+\sqrt{13}y-3z}$, $\tau_x \in O(E_3')$, we may assume that $\sqrt{13}u = x+(\pm 2+2\sqrt{13})y-6z$. Hence $E_3'' = [u, \pm(5u-9y)+x+(\pm 2\sqrt{13}-2)z, 4u\pm 2x-4y-(\pm 2-\sqrt{13})z] \simeq E_3'$. 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 $n \leqq 3$ and more than two if $n \geqq 4$.

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 $E_5(y_2) = [y_2] \perp A$. By the Proposition 4 $Q(E_4(y_1)) \not\ni 1,2$. By the Proposition 2 $Q(A) \not\ni 1$ and $Q(A) \ni 2$. 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 $n \geqq 3$.

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 $2y' = e_1+\frac{1}{2}(1+\sqrt{29})e_2+\frac{1}{2}(1-\sqrt{29})e_3$. Then $E_3(y) = [y] \perp M$ with $1 \notin Q(M)$. Clearly $Q(E_3(y')) \not\ni 1$ since $E_3(y')$ $= [y', 2e_1, \sqrt{29}e_1-e_2+e_3] \cong \begin{pmatrix} 4 & 1 & 0 \\ 1 & 4 & 2\sqrt{29} \\ 0 & 2\sqrt{29} & 31 \end{pmatrix}$.

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

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 ~~the~~ 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 $\mathfrak{p} = (\pi)$. Then a $\mathfrak{p}$-adjacent lattice to E_3 is isometric to E_3 or $E_3(x_1)$ by Proposition 1 and Lemma 5. Note that $E_3(x_1) = [e_1-e_2, x_1-e_1-2e_2+e_3, 5x_1+(1-\sqrt{33})(e_1+e_2) + (3-\sqrt{33})e_3] \cong \begin{pmatrix} 2 & 1 & 0 \\ 1 & 9 & 3\sqrt{33} \\ 0 & 3\sqrt{33} & 35 \end{pmatrix}$. Putting $x = \frac{\sqrt{33}}{3}(e_1+e_2+e_3)$, then $E_3' = E_3(x) = [e_1-e_2, x+\frac{1}{2}(3-\sqrt{33})e_1+\frac{1}{2}(1-\sqrt{33})e_2+e_3, x-2(e_1+e_2)+4e_3]$ $\cong E_3(x_1)$. To find a $\mathfrak{p}$-adjacent lattice to $E_3(x_1)$ we have only to find a $\mathfrak{p}$-adjacent lattice E_3'' to E_3'. Let $E_3'' = E_3'(y)$ with $y \in \mathfrak{p}^{-1}E_3' - E_3'$. By Lemma 2 we can assume that $y = \frac{\sqrt{33}}{11}z$ with $z \in E_3' - \mathfrak{p}E_3'$. Thus $\mathfrak{p}y \subset \omega E_3' \subset E_3$. Since $x \in E_3'$ and $B(x,y) = B(e_1+e_2+e_3,z) \in B(E_3',E_3') \subset \mathcal{O}$ we have $x+y \in E_3''$. For a vector $w \in E_3$ such that $B(w,x+y) \in \mathcal{O}$ we have $\pi B(w,x) = B(w,\pi(x+y)) - B(w,\pi y) \in \mathcal{O}$. also $\omega B(w,x) \in \mathcal{O}$. Hence $B(w,x) \in \mathcal{O}$, so $w \in E_3'$. And hence $B(w,y)$ $= B(w,x+y) - B(w,x) \in \mathcal{O}$, so $w \in E_3'(y) = E_3''$. Hence $E_3(x+y) \subset E_3''$. Since

$y = 2\omega(x+y) - (2\omega x+\pi y)$ with $2\omega x+\pi y \in E_3$ and $B(y, 2\omega x+\pi y) \in O$, we have $y \in E_3(x+y)$. For a vector $w \in E_3$ such that $B(w,x) \in O$ and $B(w,y) \in O$, we have $B(w,x+y) \in O$. Thus $E_3'' \subset E_3(x+y)$. Hence $E_3'' = E_3(u)$ with $u = x+y = \frac{1}{\sqrt{33}}(11e_1+11e_2+11e_3+3z) \in \frac{1}{\sqrt{33}}E_3$. Clearly $\sqrt{33}u \notin \mathfrak{p}E_3 \cup \omega E_3$. Write $\sqrt{33}u = \sum_{i=1}^{3} \alpha_i e_i$ with $\alpha_i \in O$. By Lemma 2 and considering the structure of $O(E_3)$, we have only to consider the following three cases:

(i) $\alpha_1 = \alpha_2 = 4$ and $\alpha_3 = 1$. Then $E_3'' = [u,\ 4u+\frac{1}{2}(1-\sqrt{33})e_1-\frac{1}{2}(1+\sqrt{33})e_2,\ 4u-\frac{1}{2}(1+\sqrt{33})e_1+\frac{1}{2}(1-\sqrt{33})e_2] \simeq E_3$.

(ii) $\alpha_1 = \alpha_2 = 2$ and $\alpha_3 = 5$. Hence $E_3'' = [u,\ 7u+\frac{1}{2}(1-\sqrt{33})e_1-\frac{1}{2}(1+\sqrt{33})e_2-\sqrt{33}e_3,\ 7u-\frac{1}{2}(1+\sqrt{33})e_1+\frac{1}{2}(1-\sqrt{33})e_2-\sqrt{33}e_3] \simeq E_3$.

(iii) $\alpha_1 = 1$, $\alpha_2 = 4$ and $\alpha_3 = 7$. Thus $E_3'' = [u,\ 4u-\sqrt{33}e_3,\ e_1+5e_2-3e_3] \simeq E_3'$.]

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

Proposition 16. Let $D = 41$. Then the class number of E_n is one if $n = 1$, two if $n = 2,3$ and more than two if $n \geqq 4$.

Proof. By ~~the~~ Proposition 6 there is a lattice G' in gen E_2 such that $1 \notin Q(G')$. Hence there are three lattices E_4, $G' \perp E_2$ and $G' \perp G'$ in gen E_4. Thus the class number of E_4 is more than two. Let $n = 3$ and $\mathfrak{p} = (\sqrt{41})$. A $\mathfrak{p}$-adjacent lattice to E_3 is isometric to E_3 or $E_3(x)$ with $x = \frac{1}{\sqrt{41}}(e_1+2e_2+6e_3)$ by ~~the~~ Propositins 1 and 4 and Lemma 3. Thus $E_3' = E_3(x) = [x, y, z] \simeq \langle 1\rangle \perp \begin{pmatrix} 5 & 2\sqrt{41} \\ 2\sqrt{41} & 5 \end{pmatrix}$ with $y = 2e_1-e_2$ and $z = \sqrt{41}(e_1+e_3) - 7x$. Take a $\mathfrak{p}$-adjacent lattice $E_3'' = E_3'(u)$ to E_3' such that $u \notin E_3'$. Write $\sqrt{41}u = \alpha x+\beta y+\gamma z$ with $\alpha, \beta, \gamma \in O$. If $\alpha \in \mathfrak{p}$, then we may assume that $\alpha = 0$ and $\gamma = 20$ by Lemma 2. Since $Q(u) \in O$, we may assume that $\beta = \pm 5-8\sqrt{41}$ by Lemma 2.

Thus $E_3'' = [x] \perp [-u, \pm 10u + (2\sqrt{41} \pm 80)y - (8 \pm 5\sqrt{41})z] \simeq E_3'$. If $\beta \in \mathfrak{p}$, then we may assume that $\alpha = 7$, $\beta = 0$ and $\gamma = 1$. Hence $u = e_1 + e_3$ and $E_3'' = E_3$. If $\gamma \in \mathfrak{p}$, we may assume that $\alpha = 6$, $\beta = 1$ and $\gamma = 0$. Thus $E_3'' = [u] \perp [14u - 2\sqrt{41}x - z] \perp [7u - \sqrt{41}x - \sqrt{41}y + 2z] \simeq E_3$. If $\alpha\beta\gamma \notin \mathfrak{p}$, then we may assume that $\gamma = 1$ and $\beta \in Z$ by Lemma 2. Note that $O(E_3')$ contains the isometries "$x \to \pm x$, $y \to 2\sqrt{41}y - 5z$, $z \to 33y - 2\sqrt{41}z$", "$x \to \pm x$, $y \to \frac{1}{2}(17-\sqrt{41})y + \frac{1}{2}(3-\sqrt{41})z$, $z \to \frac{1}{2}(7\sqrt{41}-13)y - \frac{1}{2}(17-\sqrt{41})z$" and "$x \to \pm x$, $y \to \frac{1}{2}(17+\sqrt{41})y - \frac{1}{2}(3+\sqrt{41})z$, $y \to \frac{1}{2}(13+7\sqrt{41})y - \frac{1}{2}(17+\sqrt{41})z$". Hence by Lemmas 2 and 3 we have only to consider the following two cases: (i) $\sqrt{41}u = -(-2 \pm 3\sqrt{41})x \pm 3y + z$ and (ii) $\sqrt{41}u = (10 \pm 6\sqrt{41})x \mp 30y + z$. In the case of (i) we have $E_3'' = [u, \sqrt{41}x, y \pm 13x] = [v] \perp [v_1, v_2] \simeq E_3'$, where

$$2v = (-19 \pm \sqrt{41})u - (9 \pm 3\sqrt{41})\sqrt{41}x + (5 \pm \sqrt{41})(y \pm 13x),$$

$$2v_1 = (11 \pm \sqrt{41})u + (15 \pm 3\sqrt{41})\sqrt{41}x - (7 \pm \sqrt{41})(y \pm 13x)$$

and $v_2 = 2(\pm 2 + \sqrt{41})u + (\pm 19 + 2\sqrt{41})\sqrt{41}x - (\pm 6 + \sqrt{41})(y \pm 13x)$.

Then $Q(v) = 1$. In the case of (ii) we have $E_3'' = [u, \sqrt{41}x, y \pm 15x] = [v'] \perp [v_1', v_2'] \simeq E_3'$, where

$$2v' = (-9 \pm \sqrt{41})u - (-101 \pm 11\sqrt{41})\sqrt{41}x - (-33 \pm 7\sqrt{41})(y \pm 15x),$$

$$v_1' = (21 \pm \sqrt{41})u - (236 \pm 11\sqrt{41})\sqrt{41}x + (21 \pm 15\sqrt{41})(y \pm 15x)$$

and $2v_2' = (25 \pm 17\sqrt{41})u - (273 \pm 191\sqrt{41})\sqrt{41}x + (501 \pm 11\sqrt{41})(y \pm 15x)$.

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

[1] J.Dzewas : Quadratsummen in reell-quadratischen Zahlkörpern, Math. Nachr. 21 (1960), 233-284.

[2] M.Kneser : Klassenzahlen definiter quadratischen Formen, Arch. Math. 8 (1957), 241-250.

[3] O.Nebelung: $\mathfrak{p}$-adische Darstellungsdichten binärquadratischer Formen, Dissertation, Ulm 1978.

[4] O.T.O'Meara: Introduction to quadratic forms, Berlin-Göttingen-Heidelberg, Springer-Verlag, 1963.

[5] M.Peters : Einklassige Geschlechter von Einheitsformen in totalreellen algebraischen Zahlkörpern, Math. Ann. 226 (1977), 117-120.

[6] H.Pfeuffer : Einklassige Geschlechter totalpositiver quadratischer Formen in totalreellen algebraischen Zahlkörpern, J. Number Theory 3 (1971), 371-411.

[7] H.Pfeuffer : Quadratsummen in totalreellen algebraischen Zahlkörpern, J. reine angew. Math. 249 (1971), 208-216.

[8] H.Pfeuffer : Über die reelle Spiegelungsgruppe $\mathfrak{H}_4$ und die Klassenzahl der sechsdimensionalen Einheitsform, Archiv Math. 31 (1978), 126-132.

[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),

[10] M.Pohst : Mehrklassige Geschlechter von Einheitsformen in total reellen algebraischen Zahlkörpern, J. reine angew. Math. 262/263 (1973), 420-435.

[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 $Z[\sqrt{3}]$, Archiv Math.20(1969),523-530.