

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 $\{e_1, \dots, e_n\}$. 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 “ $K = \mathbf{Q}$, $n \leq 8$ ”, “ $K = \mathbf{Q}(\sqrt{2})$, $n \leq 4$ ”, “ $K = \mathbf{Q}(\sqrt{5})$, $n \leq 4$ ”, “ $K = \mathbf{Q}(\sqrt{17})$, $n = 3$ ”, “ $K = K^{(49)}$, $n = 3$ ” or “ $K = K^{(148)}$, $n = 3$ ”, where \mathbf{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 “ $K = \mathbf{Q}(\sqrt{5})$, $n = 5, 6, 7$ ”, 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 $K = \mathbf{Q}(\sqrt{5})$ 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 ($\neq \mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{5})$, $\mathbf{Q}(\sqrt{17})$).

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

THEOREM. *In the case of real quadratic fields, the class number of E_n (with $n \geq 3$) is two if and only if*

Received June 21, 1982.

$$\begin{aligned} \mathbb{Q}(\sqrt{2}), & \quad n = 5, \\ \mathbb{Q}(\sqrt{3}), & \quad n = 3, \\ \mathbb{Q}(\sqrt{5}), & \quad n = 5, \\ \mathbb{Q}(\sqrt{13}), & \quad n = 3, \\ \mathbb{Q}(\sqrt{33}), & \quad n = 3, \\ \mathbb{Q}(\sqrt{41}), & \quad n = 3. \end{aligned}$$

The class number of E_n is a monotone increasing function of n for a fixed K ([4], 105: 1). In Section 2 we discuss some properties of adjacent lattices. In Section 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 Section 4 we treat the above exceptional cases and determine the class number by using the 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

$$A_p^n = \left\{ (a_1, \dots, a_n) \in \mathbb{Z}^n; \sum_{i=1}^n a_i^2 \equiv 0 \pmod{p}, (a_1, \dots, a_n) \not\equiv (0, \dots, 0) \pmod{p} \right\},$$

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

$$0 \leq a_1 \leq a_2 \leq \dots \leq a_n$$

and

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

for all (b_1, \dots, b_n) 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):

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

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

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:*

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

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

Let $K = \mathbf{Q}(\sqrt{D})$ be a real quadratic field over \mathbf{Q} with a square-free rational integer D and \mathfrak{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 $\mathbf{Q}(L) \subset 2\mathfrak{o}$. 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 \mathfrak{o} .

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

$$L(x) = \mathfrak{o}x + \{z \in L; B(x, z) \in \mathfrak{o}\},$$

which is called an α -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 α -adjacent lattice to L . Then $L(x)$ is unimodular. If α is prime to $2\mathfrak{o}$ or $L(x)_\mathfrak{p} \simeq L_\mathfrak{p}$ for any dyadic spot \mathfrak{p} , then an α -adjacent lattice to L belongs to $\text{gen } L$.*

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

LEMMA 3. *Let L be a unimodular lattice in V and $L(x)$ and $L(x')$ be two α -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 α -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 α , 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 $x = (\sqrt{D}/p) \sum_{i=1}^n a_i e_i$ and $(a_1, \dots, a_n) \in R_p^n \cup \{(0, \dots, 0)\}$.

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

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

since $\sqrt{D}\alpha_i \in \mathfrak{o}$ and D/p is prime to \mathfrak{p} . Put $x = (\sqrt{D}/p) \sum_{i=1}^n a_i e_i$. Then $x \in \mathfrak{p}^{-1}E_n$ and $z - x \in E_n$. We have $\sum_{i=1}^n a_i^2 \equiv 0 \pmod{p}$ since $Q(z) \in \mathfrak{o}$. Hence $Q(x) \in \mathfrak{o}$ and $(a_1, \dots, a_n) \in A_p^n$ if $x \notin E_n$. Since $-2B(x, z) = Q(z - x) - Q(x) - Q(z) \in \mathfrak{o}$ and $B(x, z) \in \mathfrak{p}^{-2}$, we have $B(x, z) \in \mathfrak{o}$. By Lemma 2 we have $E_n(z) = E_n(x)$. Considering the structure of $O(E_n)$, we may have $(a_1, \dots, a_n) \in R_p^n \cup \{(0, \dots, 0)\}$ by Lemmas 2 and 3.

§3. Special adjacent lattices to E_n

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

- 1) $\bar{A} \in \text{gen } E_n$,
- 2) A is even if $n \equiv b_1 \equiv \dots \equiv b_n \equiv 1 \pmod{2}$,
- 3) $A \in \text{gen } E_{n-1}$ unless $n \equiv b_1 \equiv \dots \equiv b_n \equiv 1 \pmod{2}$,
- 4) $A \simeq E_2$ if $n = 3$, $D \equiv 1 \pmod{4}$ and $b_i = b_j$ for some $i < j$,
- 5) $1 \notin Q(A)$ unless $n = 3$, $D \equiv 1 \pmod{4}$ and $b_i = b_j$ for some $i < j$.

Proof. (i) Suppose that D is odd. By Lemma 1 we have $\bar{A} \in \text{gen } E_n$. Let \mathfrak{p} be a dyadic spot on K . We can assume that b_1 is odd. Put $v_i = b_i e_i - b_i e_1$ for $i = 2, 3, \dots, n$. Then $A_{\mathfrak{p}} = [v_2, \dots, v_n]_{\mathfrak{p}}$ with $B(v_i, v_j) \in \mathbb{Z}$ and $\det(B(v_i, v_j)) = b_1^{2(n-2)} D \equiv 1 \pmod{2}$. The assertion (2) is clear. We shall show (3). Consider a lattice $M = [v_2, \dots, v_n]$ over \mathbb{Z} . Then $M_2 \simeq \langle 1 \rangle \perp \dots \perp \langle 1 \rangle \perp \langle D \rangle$ or $M_2 \simeq \langle 1 \rangle \perp \dots \perp \langle 1 \rangle \perp \langle D \rangle \perp \langle D \rangle \perp \langle D \rangle$ since M is not even and the Hasse symbol of M_2 takes the value $+1$, where M_2 is the $2\mathbb{Z}$ -completion of M . So $A_{\mathfrak{p}} \simeq E_{n-1_{\mathfrak{p}}}$ since $\mathfrak{o}_{\mathfrak{p}} \supset \mathbb{Z}_2$ 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 \mathfrak{p} be dyadic. Then $A_{\mathfrak{p}} = [b_1z - \sqrt{D}e_1, v_3, \dots, v_n]_{\mathfrak{p}}$ with $\det(B(v_i, v_j)) = b_1^{2(n-3)}(D - b_2^2) \equiv 1 \pmod{4}$. Thus $A_{\mathfrak{p}} \simeq [v_3, \dots, v_n]_{\mathfrak{p}} \perp \langle D - b_2^2 \rangle$. By a similar argument as in (i) we have $A_{\mathfrak{p}} \simeq E_{n-1\mathfrak{p}}$. By Lemma 1 we have $A \in \text{gen } E_{n-1}$, and so $\bar{A} \in \text{gen } E_n$.

(iii) Suppose that $n = 3$, $D \equiv 1 \pmod{4}$ and $b_1 = b_2$. Thus $b_3 \equiv 1 \pmod{2}$. Take f and g in \mathbb{Z} such that $2b_2f - b_3g = 1$. Put

$$w_1 = -(b_3f + b_2g)z + f\sqrt{D}e_3 + \frac{1}{2}(1 + g\sqrt{D})e_1 + \frac{1}{2}(-1 + g\sqrt{D})e_2$$

and $w_2 = w_1 - e_1 + e_2$. 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 $a = \sum_{i=1}^n b_i d_i \in \mathbb{Z}$, $\sum_{i=1}^n b_i c_i = 0$, $|a| \leq \frac{1}{2}D$, $c_i \in \frac{1}{2}\mathbb{Z}$, $d_i \in \frac{1}{2}\mathbb{Z}$ and $c_i - d_i \in \mathbb{Z}$ 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 $d_1/b_1 = \dots = d_n/b_n = c$ for some $c \in \mathbb{Q}$. Since the g.c.d. of b_i 's is one, we have $c \in \frac{1}{2}\mathbb{Z}$ or $c \in \mathbb{Z}$ according as $D \equiv 1 \pmod{4}$ 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 $a = d_1 = \dots = d_n = 0$. Hence $c_i \in \mathbb{Z}$ 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 \mathbb{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 $D \equiv 1 \pmod{4}$ and $d_{i'} \notin \mathbb{Z}$ for some i' . Thus $c_{i'} \notin \mathbb{Z}$. Then $\sum_{i=1}^n c_i^2 \geq \frac{1}{2}$ since $b_1 b_2 \dots b_n \neq 0$. Hence

$$\sum_{i=1}^n c_i^2 + \sum_{i < j} (b_i d_j - b_j d_i)^2 \geq \frac{1}{2} + \frac{1}{4}(n - 1) = \frac{1}{4}(n + 1) \geq 1$$

and the equality holds only when $n = 3$ and $\sum_{i=1}^n c_i^2 = \frac{1}{2}$. 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.

PROPOSITION 3. *Let $D \not\equiv 1 \pmod{4}$. Let p be an odd prime dividing D . Consider the lattice $B = E_s(y)$ with $y = (\sqrt{D}/p) \sum_{i=1}^3 a_i e_i$ and $(a_1, a_2, a_3) \in R_p^3$. Then*

- (1) $B \in \text{gen } E_3,$
- (2) $B \simeq E_1 \perp B'$ 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 $T(a_1, a_2, a_3) \geq 2$ 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 $a \in \mathbb{Z}, c_i \in \mathbb{Z}, d_i \in \mathbb{Z}, \sum_{i=1}^3 a_i c_i \equiv 0 \pmod p$ 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 $T(a_1, a_2, a_3) \geq 2.$ 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 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 $D \equiv 1 \pmod 4$ and p be a prime dividing $D.$ Consider the lattice $B = E_n(y)$ with $y = (\sqrt{D}/p) \sum_{i=1}^n a_i e_i$ and $(a_1, \dots, a_n) \in \mathbb{R}_p^n.$ Assume that $n \geq 3.$ Put $T = T(a_1, \dots, a_n)$ and $N = N(a_1, \dots, a_n).$ 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 $2 \in Q(B)$ if $D \neq p$ and $T \geq 3,$
- (5) $B \simeq E_3$ if $n = 3, D = p$ and $T \leq 2,$
- (6) $B \simeq E_1 \perp B'$ 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 $2 \sum_{i=1}^n a_i c_i \equiv 0 \pmod p.$ 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 $Y = (D/p)(1/p) \sum_{i=1}^n (aa_i + pd_i)^2.$ If $Y = 0,$ then

$a = d_i = 0$ for all i , so $c_i \in \mathbb{Z}$ for all i . Thus $X \geq T$. If $X = 0$ and $Y \neq 0$, then $c_i = 0$ for all i and $Y \geq DN/p$. If $X \neq 0$ and $Y \neq 0$, then $X + Y \geq (T/4) + (D/p)(N/4)$. Thus (3), (7), (8) and the half of (4) hold. Now suppose that $D \neq p$ and $T \geq 3$ or that $D = p$, $T \geq 3$, $N \geq 3$ and $n = 3$. Thus $X \geq \frac{3}{4}$ and $Y \geq \frac{3}{4}$. If $X = \frac{3}{4}$ with $Y = \frac{5}{4}$ or $X = \frac{5}{4}$ with $Y = \frac{3}{4}$, then we have $2 \equiv 4X - 4Y \equiv \sum_{i=1}^n (2c_i)^2 - \sum_{i=1}^n (2d_i)^2 \equiv 0 \pmod{4}$, which is a contradiction. If $X = Y = 1$, then $D = p$ and $\sum_{i=1}^n c_i^2 = 1$. Thus $D = p$ and $n \geq 4$, which is a contradiction. Hence (9) and the rest of (4) hold. If $n = 3$, $D \neq p$ and $T = 1$, then $a_1 = 0$ 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 $T \leq 2$. Then $N = 1$. If $T = 1$, then $B = [e_1] \perp [y] \perp [y'] \simeq E_3$ with $y' = (1/\sqrt{p})(a_3e_2 - a_2e_3)$. 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 $D \equiv 3 \pmod{4}$. Consider the lattice $C = E_3(x) = [e_3] \perp C'$ with $x = \frac{1}{2}(e_1 + \sqrt{D}e_2)$. Then*

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

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 $D \equiv 3 \pmod{8}$, 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 $D \equiv 7 \pmod{8}$, 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 $D \equiv 5 \pmod{12}$. 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) $G \in \text{gen } E_3$ and $G' \in \text{gen } E_{23}$,
- (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 $p \equiv 1 \pmod{12}$. Then the number of the classes in A_p^3 whose type is six is one or zero according as*

$p \equiv 1 \pmod{24}$ or $p \equiv 13 \pmod{24}$. Let $(a_1, a_2, a_3) \in R_p^3$ with $T = T(a_1, a_2, a_3) \geq 3$ and $N(a_1, a_2, a_3) = 2$. Put $x = (1/\sqrt{p})(a_1e_1 + a_2e_2 + a_3e_3)$. 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 $0 \equiv \sum_{i=1}^3 b_i^2 \equiv 2(b_1 + b_2)^2 + 3b_1^2 \pmod{p}$. So $(-6/p) = 1$, i.e., $p \equiv 1 \pmod{24}$. If $p \equiv 1 \pmod{24}$, then there is an integer c such that $c^2 \equiv -6 \pmod{p}$. Hence $\pm c(b_1 + b_2) \equiv 3b_1 \pmod{p}$. 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 $a \in \mathbf{Z}$, $|a| < \frac{1}{2}p$, $c_i \in \frac{1}{2}\mathbf{Z}$, $d_i \in \frac{1}{2}\mathbf{Z}$, $c_i - d_i \in \mathbf{Z}$, $2 \sum_{i=1}^3 a_i c_i \equiv 0 \pmod{p}$. Then $Q(u) = X + Y + (2/\sqrt{p}) \sum_{i=1}^3 c_i(aa_i + pd_i)$, where $X = \sum_{i=1}^3 c_i^2$ and $Y = (1/p) \sum_{i=1}^3 (aa_i + pd_i)^2$. Hence we have one of the following:

- (i) $X = 0$ and $Y = 2$,
- (ii) $X = \frac{5}{4}$ and $Y = \frac{3}{4}$,
- (iii) $X = \frac{3}{2}$ and $Y = \frac{1}{2}$.

In the case (ii) we have $1 \equiv \sum_{i=1}^3 (2c_i)^2 \equiv \sum_{i=1}^3 (2d_i)^2 \equiv \sum_{i=1}^3 (2aa_i + 2pd_i)^2 = 3p \equiv 3 \pmod{4}$. 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 $c^2 + 6 \equiv 0 \pmod{p}$ by the argument used above since $X = \frac{6}{4}$. Since T must be five we have $c \equiv \pm 1, \pm 2, \pm 3, \pm 6$ or $\pm 9 \pmod{p}$, which is a contradiction to the fact that p divides $c^2 + 6$. In the case (i) we have $c_i = 0$ and $d_i \in \mathbf{Z}$ for all i . Hence we can write $u_1 = ax + \sqrt{p} \sum_{i=1}^3 d_i e_i = (1/\sqrt{p}) \sum_{i=1}^3 f_i e_i$ and $u_2 = a'x + \sqrt{p} \sum_{i=1}^3 d'_i e_i = (1/\sqrt{p}) \sum_{i=1}^3 f'_i e_i$ with $a, a', d_i, d'_i, f_i, f'_i \in \mathbf{Z}$. Thus $f_i \equiv aa_i \pmod{p}$ and $f'_i \equiv a'a_i \pmod{p}$. Hence $f_i f'_j - f_j f'_i \equiv 0 \pmod{p}$. 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., $a_1 h_{23} + a_2 h_{31} + a_3 h_{12} \equiv 0 \pmod{p}$. This implies that $T \leq 3$. This is a contradiction.

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 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 gen E_3 such that $L \neq E_3$, $M \neq E_3$ and $L \neq M$.

(i) Let $D \equiv 2 \pmod 4$. For L we take the lattice A in Proposition 2 if $D = 10$. If $D \neq 10$, then there is an odd prime $q (\neq 5)$ dividing D . By 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 Proposition 3. Then put $L = B$ if $D \neq 10$. Next take an odd prime p dividing D . If $p \equiv 1 \pmod 4$, 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 Proposition 3. If $p \equiv 3 \pmod 4$, then we can consider the lattice \bar{A} in Proposition 2. Then put $M = B$ or $M = \bar{A}$ according as $p \equiv 1 \pmod 4$ or $p \equiv 3 \pmod 4$. Note that $1 \notin Q(L)$ and $M \simeq E_1 \perp M'$ with $1 \notin Q(M')$.

(ii) Let $D \equiv 3 \pmod 8$. For L we take a lattice $\bar{A} \simeq E_1 \perp A$ with an even lattice A in 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 Proposition 5.

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

(iv) Let $D \equiv 1 \pmod 4$ and not a prime. If no prime divisor of D is congruent to $7 \pmod 8$, then by 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 $T(a'_1, a'_2, a'_3) \geq 2$ 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 Proposition 4. If D has a prime divisor $p \equiv 7 \pmod 8$, 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 $Q(B) \not\equiv 1$ in 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 $D \equiv 1 \pmod 4$ and $p \equiv 3 \pmod 4$. We have $b_i \neq b_j$ whenever $i \neq j$ since $(-2/p) = -1$. Hence we can consider a lattice $\bar{A} = E_1 \perp A$ with $1 \notin Q(A)$. Put $M = \bar{A}$.

(v) Let D be a prime $p \equiv 1 \pmod{12}$. 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 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 $p \equiv 1 \pmod{24}$. 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 $p \equiv 13 \pmod{24}$. There is an element $(a_1, a_2, a_3) \in R_p^3$ whose type is more than three by Proposition 1. For M we take the lattice B for (a_1, a_2, a_3) in 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 Proposition 7.

(vi) Let D be a prime $p \equiv 5 \pmod{12}$. For L we take the lattice A with $1 \notin Q(A)$ in Proposition 2. For M we take the lattice $G = E_1 \perp G'$ 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

$$J^{\mathfrak{p}} = \{j = (j_q) \in J; j_q \text{ is a unit in } \mathcal{O}_q \text{ for all finite spot } q \neq \mathfrak{p}\}.$$

Put $V = KE_n$ 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 $K^* \rightarrow J$. Recall Theorem 104:9 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 $M_{\mathfrak{q}} = E_{n_{\mathfrak{q}}}$ for all finite spot $\mathfrak{q} \neq \mathfrak{p}$.*

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

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 $E_6, E_6((1/\sqrt{2})(e_1 + \dots + e_4))$ and $E_6((1/\sqrt{2})(e_1 + \dots + e_5))$ in $\text{gen } E_6$, any two of which are not isometric. Let $n = 5$. Take $p = (\sqrt{2})$ and a p -adjacent lattice $E_5(x)$ in $\text{gen } E_5$. Write $x = (1/\sqrt{2}) \sum_{i=1}^5 \alpha_i e_i$. Note that $O(E_5)$ contains all permutations of $\{e_1, \dots, e_5\}$. And note that $Q(x) \equiv 0$ or $1 \pmod{2}$ since $E_5(x) \in \text{gen } E_5$. By Lemmas 2 and 3 we have only to consider the following three cases: (i) $\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = \alpha_5 = 0$. 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 $u = (1/\sqrt{2})(e_1 + \dots + e_4)$. Hence a \mathfrak{p} -adjacent lattice to E_5 in $\text{gen } E_5$ 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 $\text{gen } E_5$ and write $\sqrt{2}y = w + \alpha e_5$ with $\alpha \in \mathfrak{o}$ and $w \in E_4^0$. Since $Q(y) \in \mathfrak{o}$ and E_4^0 is even, we have $\alpha \in \mathfrak{p}$. By Lemma 2 we have $E'_5(y) = E'_5((1/\sqrt{2})w) = E_4^0((1/\sqrt{2})w) \perp [e_5]$. Hence we may write $\sqrt{2}y = au + \sum_{i=1}^4 \alpha_i e_i$ where $\alpha_i \in \mathfrak{o}$, $a \in \{0, 1\}$ and $\sum_{i=1}^4 \alpha_i \equiv 0 \pmod{\sqrt{2}}$. Note that $Q(y) \equiv 0$ or $1 \pmod{2}$ 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) $\alpha_1 = \alpha_2 = \alpha_3 = \alpha_4 = 0$. 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 $E'_5(y) = E_4^0(y) \perp [e_5] = E_2((1/\sqrt{2})(e_1 + e_2)) \perp E_2((1/\sqrt{2})(e_3 + e_4)) \perp [e_5] \simeq E_5$. (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 $\sqrt{2}\tau_{e_1}y = u + (-\alpha_1 - \sqrt{2})e_1 + \alpha_2 e_2 + \dots$. Hence we may assume that $\alpha_i \equiv 0 \pmod{2}$ or $\alpha_i \equiv 1 \pmod{2}$. 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 $\text{gen } E_5$ 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 $x = (1/\sqrt{5})(e_1 + \dots + e_5)$, $y_1 = (1/\sqrt{5})(e_1 + e_2 + 2e_3 + 2e_4)$ and $x_1 = (1/\sqrt{5})(e_1 + e_2 + e_3 + 2e_4 + 2e_5 + 2e_6)$. Consider the lattice $E'_5 = E_5(x) = [x] \perp E_4^0$. Then E_4^0 is even. If $n = 6$, then we have three lattices $E_6, E_6(x)$ and $E'_6 = E_6(x_1)$ in $\text{gen } E_6$. 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 $y = (1/\sqrt{5}) \sum_{i=1}^5 a_i e_i$ with $(a_1, \dots, a_5) \in R_5^5$. Hence $y \in \{0, x, (1/\sqrt{5})(e_1 + 2e_2), y_1\}$. Thus $E_5(0) = E_5$, $E_5(x) = E'_5$ and $E_5((1/\sqrt{5})(e_1 + 2e_2)) \simeq E_5$. By 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 $\sqrt{5}z = ax + \sum_{i=1}^5 \alpha_i e_i$

where $a = 0$ or 1 , $\alpha_i = a_i + b_i\sqrt{5} \in Z[\sqrt{5}]$ and $\sum_{i=1}^5 a_i \equiv 0 \pmod{5}$. If $a = 0$, then we have only to consider the following three cases by Lemmas 2 and 3:

(i) $\alpha_1 = \dots = \alpha_5 = 0$. Then $z = \sum_{i=1}^5 b_i e_i$, so $E'_5(z) = E'_5$ or $E'_5(z) = E_5$ according as $\sum_{i=1}^5 b_i \equiv 0 \pmod{5}$ or not.

(ii) $\alpha_1 = \dots = \alpha_5 = 1$. Thus $z = x + \sum_{i=1}^5 b_i e_i$ with $\sum_{i=1}^5 b_i \equiv 0 \pmod{5}$, so $z \in E'_5$. Hence $E'_5(z) = E'_5$.

(iii) $\alpha_1 = 1, \alpha_2 = -1, \alpha_3 = 2, \alpha_4 = -2, \alpha_5 = b_1 = \dots = b_4 = 0$ 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 $E'_5(z) = [z_0, z_1, \dots, z_4] \simeq E_5$, where $z_0 = z + \bar{\zeta}e_3 + \zeta e_4 - e_5, z_1 = z + x + \bar{\zeta}e_1 + \zeta e_3 - e_5, z_2 = z + 2x + \bar{\zeta}e_1 - \sqrt{5}e_3 - \zeta e_5, z_3 = z - 2x + \zeta e_2 + \sqrt{5}e_4 - \bar{\zeta}e_5$ 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 $\{e_1, \dots, e_5\}$):

(iv) $\alpha_1 = \dots = \alpha_4 = 0$ 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 $w = 3x - \sqrt{5}(e_3 + e_4 + e_5)$.

(ix) $\alpha_1 = 2, \alpha_2 = 1, \alpha_3 = -1, \alpha_4 = -2$ and $\alpha_5 = 2\sqrt{5}$. Then we have $E'_5(z) = [2z + x - \sqrt{5}e_1 - \zeta e_2 - \bar{\zeta}e_4 - 4e_5, 2z - 2x - \zeta e_1 + \sqrt{5}e_3 + \sqrt{5}e_4 + (\zeta - 5)e_5, 2z + 2x - \sqrt{5}e_1 - \sqrt{5}e_2 - \bar{\zeta}e_4 - (\zeta + 4)e_5, 2z - x - \zeta e_1 - \bar{\zeta}e_3 + \sqrt{5}e_4 - 4e_5, 2z - \sqrt{5}e_1 - \zeta e_2 - \bar{\zeta}e_3 + \sqrt{5}e_4 - 4e_5] \simeq E_5$.

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 $n \leq 2$, 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 $\sqrt{13}y_2 = e_1 + 3e_2 + 4e_3$. By Proposition 4 $Q(E_4(y_1)) \ni 1$, $Q(E_3(y_2)) \ni 1$ 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 $p \in (\sqrt{13})$. Take a p -adjacent lattice $E'_3 = E_3(x)$ to E_3 . By Lemma 5 and Proposition 4(5) we may consider $\sqrt{13}x = e_1 + 3e_2 + 4e_3$. Thus

$$Q(E'_3) \ni 1 \quad \text{and} \quad E'_3 = [x, y, z] \simeq \begin{pmatrix} 2 & 0 & 1 \\ 0 & 3 & \sqrt{13} \\ 1 & \sqrt{13} & 5 \end{pmatrix},$$

where $y = e_1 + e_2 - e_3$ and $z = 6x - \sqrt{13}(e_2 + 2e_3)$. Next consider a p -adjacent lattice $E''_3 = E'_3(u)$ to E'_3 with $\sqrt{13}u = \alpha x + \beta y + \gamma z \in E'_3 - pE'_3$. If $\beta \in p$, then we may assume that $\beta = 0$ and $\alpha = 1$ by Lemma 2. Thus we may assume that $\gamma = 2$ or $\gamma = -5$ since $Q(u) \in \mathfrak{o}$ 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 $\beta \notin p$. Then by Lemma 2 we may assume that α and $\beta \in \mathbb{Z}$ such that $|\alpha| \leq 6$ and $|\beta| \leq 6$ and that $\beta \equiv 2 \pmod{\sqrt{13}}$. 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 $n \leq 3$ 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 $E_5(y_2) = [y_2] \perp A$. By Proposition 4 $Q(E_4(y_1)) \ni 1, 2$. By Proposition 2 $Q(A) \ni 1$ and $Q(A) \ni 2$. Hence the class number of E_4 is more than two. Let $n = 3$. Then by Lemma 5 and 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 $2y' = e_1 + \frac{1}{2}(1 + \sqrt{29})e_2 + \frac{1}{2}(1 - \sqrt{29})e_3$. Then $E_3(y) = [y] \perp M$ with $1 \notin Q(M)$. Clearly $Q(E_3(y')) \ni 1$ since

$$E_3(y') = [y', 2e_1, \sqrt{29}e_1 - e_2 + e_3] \simeq \begin{pmatrix} 4 & 1 & 0 \\ 1 & 4 & 2\sqrt{29} \\ 0 & 2\sqrt{29} & 31 \end{pmatrix}.$$

PROPOSITION 15. *Let $D = 33$. Then the class number of E_n is one if $n \leq 2$, 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 $x_1 = (\sqrt{33}/11)(e_1 + e_2 + 3e_3)$ and $x_2 = (\sqrt{33}/11)(e_1 + e_2 + 2e_3 + 4e_4)$. 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 $\mathfrak{p} = (\pi)$. 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

$$E_3(x_1) = [e_1 - e_2, x_1 - e_1 - 2e_2 + e_3, 5x_1 + (1 - \sqrt{33})(e_1 + e_2) + (3 - \sqrt{33})e_3] \\ \simeq \begin{pmatrix} 2 & 1 & 0 \\ 1 & 9 & 3\sqrt{33} \\ 0 & 3\sqrt{33} & 35 \end{pmatrix}.$$

Putting $x = (\sqrt{33}/3)(e_1 + e_2 + e_3)$, then $E'_3 = E_3(x) = [e_1 - e_2, x + \frac{1}{2}(3 - \sqrt{33})e_1 + \frac{1}{2}(1 - \sqrt{33})e_2 + e_3, x - 2(e_1 + e_2) + 4e_3] \simeq E_3(x_1)$. 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 $y = (\sqrt{33}/11)z$ 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 $B(x, y) = B(e_1 + e_2 + e_3, z) \in B(E'_3, E'_3) \subset \mathfrak{o}$ we have $x + y \in E'_3$. For a vector $w \in E_3$ such that $B(w, x + y) \in \mathfrak{o}$ we have $\pi B(w, x) = B(w, \pi(x + y)) - B(w, \pi y) \in \mathfrak{o}$, also $\omega B(w, x) \in \mathfrak{o}$. Hence $B(w, x) \in \mathfrak{o}$, so $w \in E'_3$. And hence $B(w, y) = B(w, x + y) - B(w, x) \in \mathfrak{o}$, 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 $B(y, 2\omega x + \pi y) \in \mathfrak{o}$, we have $y \in E_3(x + y)$. For a vector $w \in E_3$ such that $B(w, x) \in \mathfrak{o}$ and $B(w, y) \in \mathfrak{o}$, we have $B(w, x + y) \in \mathfrak{o}$. Thus $E''_3 \subset E_3(x + y)$. Hence $E''_3 = E_3(u)$ with $u = x + y = (1/\sqrt{33})(11e_1 + 11e_2 + 11e_3 + 3z) \in (1/\sqrt{33})E_3$. 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 $\alpha_i \in \mathfrak{o}$. 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 $n \geq 4$.*

Proof. By 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 $x = (1/\sqrt{41})(e_1 + 2e_2 + 6e_3)$ by Propositions 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 $\alpha, \beta, \gamma \in \mathfrak{o}$. If $\alpha \in \mathfrak{p}$, then we may assume that $\alpha = 0$ and $\gamma = 20$ by Lemma 2. Since $Q(u) \in \mathfrak{o}$, 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

$$\begin{aligned} & "x \rightarrow \pm x, y \rightarrow 2\sqrt{41}y - 5z, z \rightarrow 33y - 2\sqrt{41}z", \\ & "x \rightarrow \pm x, y \rightarrow \frac{1}{2}(17 - \sqrt{41})y + \frac{1}{2}(3 - \sqrt{41})z, \\ & \quad z \rightarrow \frac{1}{2}(7\sqrt{41} - 13)y - \frac{1}{2}(17 - \sqrt{41})z" \end{aligned}$$

and

$$\begin{aligned} & "x \rightarrow \pm x, y \rightarrow \frac{1}{2}(17 + \sqrt{41})y - \frac{1}{2}(3 + \sqrt{41})z, \\ & \quad y \rightarrow \frac{1}{2}(13 + 7\sqrt{41})y - \frac{1}{2}(17 + \sqrt{41})z". \end{aligned}$$

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

$$\begin{aligned} 2v &= (-19 \pm \sqrt{41})u - (9 \pm 3\sqrt{41})\sqrt{41}x + (5 \pm \sqrt{41})(y \pm 13x). \\ 2v_1 &= (11 \pm \sqrt{41})u + (15 \pm 3\sqrt{41})\sqrt{41}x - (7 \pm \sqrt{41})(y \pm 13x) \end{aligned}$$

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

$$\begin{aligned} 2v' &= (-9 \pm \sqrt{41})u - (101 \pm 11\sqrt{41})\sqrt{41}x - (-33 \pm 7\sqrt{41})(y \pm 15x), \\ v'_1 &= (21 \pm \sqrt{41})u - (236 \pm 11\sqrt{41})\sqrt{41}x + (21 \pm 15\sqrt{41})(y \pm 15x) \end{aligned}$$

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.*, **3** (1957), 241–250.
- [3] O. Nebelung, 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] —, Quadratsummen in totalreellen algebraischen Zahlkörpern, *J. reine angew. Math.*, **249** (1971), 208–216.
- [8] —, Über die reelle Spiegelungsgruppe \mathfrak{k}_4 und die Klassenzahl der sechsdimensionalen Einheitsform, *Arch. Math.*, **31** (1978), 126–132.
- [9] —, 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 $Z[\sqrt{3}]$, Arch. Math., **20** (1969), 523–530.

Department of Mathematics
Kobe University
Nada-ku, Kobe 657
Japan