PROPER EMBEDDING INTO A UNIT LATTICE

YOSHIO MIMURA

0. Introduction. An *n*-dimensional quadratic lattice is a free module of rank *n* over the rational integer ring \mathbf{Z} , which is endowed with a symmetric bilinear form *B*. Let E_n be a unit lattice, that is an *n*-dimensional quadratic lattice which has an orthonormal basis with respect to *B*, i.e.,

$$E_n = \mathbf{Z}e_1 + \dots + \mathbf{Z}e_n, \quad B(e_i, e_j) = \delta_{ij},$$

where δ_{ij} is the Kronecker delta. Let A be a positive integer. A sublattice F of E_n is an r-frame of scale A if

$$F = \mathbf{Z}f_1 + \cdots + \mathbf{Z}f_r, \quad B(f_i, f_j) = A\delta_{ij}.$$

A frame F in E_n is proper if $B(F, e_j) \neq \{0\}$ for each j. In this situation we have a problem:

(*) When does E_n contain a proper r-frame of scale A?

We shall give a complete answer in the case of r = 2. Why proper? The Siegel Mass Formula can answer the question: When does E_n contain an *r*-frame of scale A?

This problem leads to diophantine equations in the following:

(#) E_n contains a proper 1-frame of scale A if and only if there are integers x_1, \ldots, x_n in Z satisfying

$$x_1^2 + \dots + x_n^2 = A, \quad x_1 \neq 0, \dots, x_n \neq 0;$$

(##) E_n contains a proper 2-frame of scale A if and only if there are integers $x_1, \ldots, x_n, y_1, \ldots, y_n$ in **Z** satisfying

$$x_1^2 + \dots + x_n^2 = y_1^2 + \dots + y_n^2 = A, \quad x_1 y_1 + \dots + x_n y_n = 0,$$

$$x_1 \neq 0 \text{ or } y_1 \neq 0, \dots, x_n \neq 0 \text{ or } y_n \neq 0.$$

Received by the editors on October 1, 1986.

Copyright ©1989 Rocky Mountain Mathematics Consortium

T. Ono proposed an interesting problem - a skew hanging of picture frames - which leads to the above problem (*) in the case of n = 3 and r = 2.

We can write $A = 2^e A_1 A_3$, where $p \equiv j \mod 4$ for all prime divisors p of $A_j (j = 1, 3)$.

1. 1-frames. This case is to characterize the set S_n of sums of n non-zero squares by (#).

THEOREM 1. Let $n \neq 3$. E_n contains a proper 1-frame of scale A if and only if one of the following is satisfied:

(1) n = 1, A is a square;

- (2) n = 2, A_3 is a square, e is odd or $A_1 > 1$;
- (3) $n = 4, A \neq 1, 3, 5, 9, 11, 17, 29, 41, 2 \cdot 4^k, 6 \cdot 4^k, 14 \cdot 4^k;$
- (4) $n = 5, A \neq 1, 2, 3, 4, 6, 7, 9, 10, 12, 15, 18, 33;$
- (5) $n \ge 6, A \ne 1, 2, \dots, n-1, n+1, n+2, n+4, n+5, n+7, n+10, n+13.$

PROOF. It is classical for n = 1, 2. Assume $n \ge 4$. All the conditions are clearly necessary by direct calculations. In case n =4, it suffices to show that $A \in S_4$ if $A \not\equiv 0 \mod 8$ and $A \neq 4$ 1, 3, 5, 9, 11, 17, 29, 41, 2, 6, 14. When $A \not\equiv 1 \mod 4$, we define an integer C by $A = a^2 + C$, where a = 1 (if $A \equiv 4, 7 \mod 8$), a = 2(if $A \equiv 2 \mod 8$), and a = 4 (if $A \equiv 3, 6 \mod 8$). When $A \equiv 3$ 1 mod 4, we define an integer C by $A = a^2 + 4C$, where a = 1(if $A \equiv 13, 25 \mod 32$), a = 3 (if $A \equiv 1, 21 \mod 32$), a = 5 (if $A \equiv 5, 17 \mod 32$), and a = 7 (if $A \equiv 9, 29 \mod 32$). Then C is a positive integer with $C \equiv 3, 6 \mod 8$; Hence we have $C \in S_3$ by a classical result. Therefore $A \in S_4$. In case $n \geq 5$, we use induction on n. Put $T_n = \{n, n+3, n+6, n+8, n+9, n+11, n+12\} \cup \{m \in \mathbb{Z} : m \ge n+14\}.$ Take $A \in T_5$ with $A \neq 33$. If $A \leq 45$, then we have $A \in S_5$ by direct calculations. If A > 45, then either $A - 1^2$ or $A - 2^2$ is an odd positive integer > 41. Hence it is a sum of four non-zero squares from the case of n = 4. Then we have $A \in S_5$. Take $A \in T_n$ with $n \ge 6$. Then we have $A - 1^2 \in T_{n-1}$. By the inductive hypothesis, we have $A-1^2 \in S_{n-1}$ (except n = 6 and A = 34). Thus $A \in S_n$ (and

 $34 = 2^2 + 2^2 + 2^2 + 2^2 + 3^2 + 3^2$).

REMARK. In case n = 3, the problem is: what A is a sum of three non-zero squares? This is a famous and open problem. We may assume that $A \equiv 1, 2, 5 \mod 8$ (because we know the following: $A \in S_3$ if and only if $4A \in S_3$, $A \in S_3$ if $A \equiv 3, 6 \mod 8$, $A \notin S_3$ if $A \equiv 7 \mod 8$). Under the notation $A = 2^e A_1 A_3$, we may assume that A_3 is a square (because we know that $A \in S_3$ if A_3 is not a square). If A contains an odd square > 1, then we have

$$A = u^{2} + v^{2} + w^{2}$$
 or $A = u^{2} = v^{2} + w^{2}$

for some non-zero integers u, v, w by Theorem 2 (in case n = 3) in the next section. If A is the first, then we have $A \in S_3$. If A is the second, then u contains a prime $p \equiv 1 \mod 4$ since $vw \neq 0$. First suppose that $A \neq p^2$. The same argument implies that $A/p^2 \in S_3$ or $A/p^2 = v_1^2 + w_1^2$ with $v_1w_1 \neq 0$. Hence $A \in S_3$ or $A = (pv_1)^2 + (pw_1)^2 =$ $(pv_1)^2 + ((s^2 - t^2)w_1)^2 + (2stw_1)^2 \in S_3$, since we can write $p = s^2 + t^2$ with s > t > 0. Let $A = p^2 = (s^2 - t^2)^2 + (2st)^2$. If $s \equiv 0$ or $t \equiv 0$ or $s^2 \equiv t^2 \mod 5$, then we have $A \in S_3$ since $(5r)^2 = (3r)^2 + (4r)^2$. Otherwise, we have $s^2 \equiv -t^2 \mod 5$, so p = 5. We note that $25 \notin S_3$. After all we may consider the case where A is square-free, A > 1, and $p \equiv 1 \mod 4$ for all prime divisors of A. In this case, we have the known formulas

$$\#\{(a,b)\in \ \mathbf{Z}^2: a^2+b^2+c^2=A\}=2^{t+1}$$

 and

$$\#\{(a,b,c) \in \mathbf{Z}^3 : a^2 + b^2 + c^2 = A\} = 12h(-A) \ge 12 \cdot 2^{t-1},$$

where t is the number of distinct primes in 4a, and h(-A) is the ideal class number of quadratic field $\mathbf{Q}(\sqrt{-A})$. Hence we have $A \in S_3$ if and only if $h(-A) = 2^{t-1}$. This result shows that $A \in S_3$ if and only if each genus contains only one ideal class in the quadratic field $\mathbf{Q}(\sqrt{-A})$. A numerical example shows that if A < 1376256, then it occurs if and only if A = 1, 2, 5, 10, 13, 25, 37, 58, 85, 130.

2. 2-frames.

THEOREM 2. E_n contains a proper 2-frame of scale A if and only if one of the following is satisfied:

- (1) n = 2, A_3 is a square;
- (2) n = 3, A_3 is a square, A contains an odd square > 1;
- (3) $n \ge 4$, n is even, $A \ge n/2$;
- (4) $n = 5, A \neq 1, 2, 3, 5, 6, 9, 21;$
- (5) $n = 7, A \neq 1, 2, 3, 4, 7;$
- (6) $n \ge 9$, *n* is odd, $A \ge (n+3)/2$.

PROOF. Consider the Gaussian integer ring $\Gamma = \mathbf{Z}[i]$ with $i = \sqrt{-1}$. Putting $z_j = x_j + y_j i$ in (##), the lattice E_n contains a proper 2-frame of scale A if and only if

(\$) there are Gaussian integers $z_1, \ldots, z_n \in \Gamma$ satisfying

$$z_1^2 + \dots + z_n^2 = 0$$
, $N(z_1) + \dots + N(z_n) = 2A$, $z_1 \neq 0, \dots, z_n \neq 0$,

where $N(z) = z\overline{z}$ is the norm of z. If the condition (\$) holds, then we have $n \ge 2$.

(1). Case n = 2. By (\$), we have $z_2^2 = -z_1^2$, so $N(z_1) = N(z_2)$. Hence $A = N(z_1)$, which shows A_3 is a square. Conversely assume that A_3 is a square. Then we have $A = N(z_1)$ with $0 \neq z_1 \in \Gamma$. Putting $z_2 = iz_1$, we see that the condition (\$) holds.

(2). Case n = 3. Assume that the condition (\$) holds. By δ we denote a G.C.D. of z_1, z_2 and z_3 . Put $z_j = \delta w_j$ with $w_j \in \Gamma$. Take a prime $\pi = 1 + i$. We may suppose that $w_1 \equiv w_2 \equiv 1$, $w_3 \equiv 0 \mod \pi$, since $w_1^2 + w_2^2 + w_3^2 \equiv 0$. Then we have $w_3^2 \equiv 0 \mod 4$, by noticing that $w_1^2 \equiv \pm 1$, $w_2^2 \equiv \pm 1$, $w_3^2 \equiv 0$, $2i \mod 4$ and $w_1^2 + w_2^2 + w_3^2 \equiv 0 \mod 4$. Hence we see that

$$(iw_1 + w_2)/2 = \beta^2 \varepsilon, \quad (iw_1 - w_2)/2 = \gamma^2 \varepsilon^{-1}, \quad w_3 = 2\beta\gamma$$

with $\beta, \gamma \in \Gamma$ and $\varepsilon \in \{\pm 1, \pm i\}$. Hence we have

$$w_1 = -i(\beta^2 \varepsilon + \gamma^2 \varepsilon^{-1}), \quad w_2 = \beta^2 \varepsilon - \gamma^2 \varepsilon^{-1},$$

whence $2A = N(\delta)(N(w_1) + N(w_2) + N(w_3)) = 2N(\delta)(N(\beta) + N(\gamma))^2$. Using the fact

$$1 \equiv w_2 \equiv \beta^2 - \gamma^2 \equiv \beta - \gamma \mod \pi \text{ and } \beta \gamma \neq 0,$$

we see that $N(\beta) + N(\gamma)$ is odd and greater than 1, and that A contains an odd square > 1. We note that $N(\delta)$ is of form $2^k a_1 a_3$ with a_3 a square (see the end of §0).

Conversely assume that A_3 is a square and A contains an odd square $a^2 > 1$. Thus we can write $A = N(\delta)a^2$ with $\delta \in \Gamma$. A classical result shows that $a = x_1^2 + x_2^2 + x_3^2 + x_4^2$ with $x_1, x_2, x_3, x_4 \in \mathbb{Z}$ and $x_1x_3 \neq 0$. Put $\beta = x_1 + ix_2$, $\gamma = x_3 + ix_4$, $w_1 = -i(\beta^2 + \gamma^2)$, $w_2 = \beta^2 - \gamma^2$, $w_3 = 2\beta\gamma$ and $z_j = \delta w_j$. Then we have $w_1w_2w_3 \neq 0$ from the fact that a is odd. Hence the condition (\$) holds.

(3). Case $n \ge 4$, even. The necessity is clear. Assume that $2A \ge n$. Then we have $A+2-n/2 = a_1^2+a_2^2+a_3^3+a_4^2$ with $a_1, a_2, a_3, a_4 \in \mathbb{Z}$ and $a_1a_2 \ne 0$, since $A+2-n/2 \ge 2$. Put $z_1 = a_1 + ia_3, z_2 = a_2 + ia_4, z_3 = a_3 - ia_1, z_4 = a_4 - ia_2, z_5 = \cdots = z_m = 1$ and $z_{m+1} = \cdots = z_n = i$, where m = 2 + n/2. Thus the condition (\$) holds.

(4). Case n = 5. The necessity is clear. We shall show the sufficiency. By Lemma 4 below, if $A \neq 5, 7, 9, 15, 21, 39, 4^k, 2 \cdot 4^k, 3 \cdot 4^k, 6 \cdot 4^k$, then we can write

$$A = a^2 + b^2 + g^2(c^2 + d^2),$$

where $a, b, c, d \in \mathbb{Z}$, $ac \neq 0$, g > 1 and g odd. From the case n = 3, there are z_3, z_4, z_5 in Γ satisfying

$$z_3^2 + z_4^2 + z_5^2 = 0$$
, $N(z_3) + N(z_4) + N(z_5) = 0$, $z_3 z_4 z_5 \neq 0$.

Putting $z_1 = a + bi$ and $z_2 = b - ai$, we see that the condition (\$) holds.

We write $z = (z_1, z_2, z_3, z_4, z_5)$ shortly. If A = 7, 15, 39, then we put z = (2, 1+2i, 1-i, 1-i, i), (3+i, 2-2i, 1+i, 1, 3i), (6, 1-3i, 1+2i, 1+i, 5i) respectively. If $A = 4^k, 2 \cdot 4^k, 3 \cdot 4^k, 6 \cdot 4^k$ with $k \ge 1$, then we put $z = 2^{k-1}(2, i, i, i, i), 2^{k-1}(2-2i, 1+i, 1+i, 1+i, 1+i), 2^{k-1}(3, 1, 1+2i, 1-2i, 2i), 2^{k-1}(4-2i, 2+3i, 2+i, i, 3i)$ respectively. Thus (\$) holds.

(5). Case n = 7. The necessity is clear. If $A - 1 \neq 0, 1, 2, 3, 5, 6, 9, 21$, then (\$) holds, using the z_j 's in the case n = 5 for A - 1 and putting $z_6 = 1, z_7 = i$. If $A - 2 \neq -1, 0, 1, 2, 3, 5, 6, 9, 21$, then we use the z_j 's in the case n = 5 for A - 2 and put $z_6 = 1 + i, z_7 = 1 - i$. Hence if $A \neq 1, 2, 3, 4, 7$, then (\$) holds. We shall give another proof without using the case n = 5. If A = 5, 6, 8, 9, 10, then we put z = (1, 1, 1, 1, 1, i, 2i), (1, 1, 1, 1, 2i, 1 + i, 1 - i), (1, 1, 1, 1, 2i, 2i, 2), (1, 1, 1, 1, 1, 2, 3i), (1, 1, 1 + i, 1 - i, 1 + 2i, 1 - 2i, 2) respectively. If $A \ge 11$ then we put $z = (a_1 + a_3i, a_2 + a_4i, -a_1i)$, $a_4 - a_i, 2 + 2i, 2 - i, 1 - 2i)$, where $A - 9 = a_1^2 + a_2^2 + a_3^2 + a_4^2$ with $a_1a_2 \neq 0$.

(6). Case $n \ge 9$, odd. If (\$) holds, then we have $2A \ge n$, so $2A \ge n + 1$. If 2A = n + 1, then we may suppose that $N(z_1) = 2, N(z_2) = \cdots = N(z_n) = 1$. Hence $z_1 = \pm 1 \pm i$ and $z_j = \pm 1$ $(j \ge 2)$, which contradicts the fact $z_1^2 + \cdots + z_n^2 = 0$. Thus $A \ge (n+3)/2$. We shall prove the sufficiency. If A = (n+3)/2, then we put $z_1 = 2i, z_2 = \cdots = z_{(n-3)/2} = i$, and $z_{(n-1)/2} = \cdots = z_n = 1$. If A = (n+5)/2 then we put $z_1 = 2i, z_2 = 1 + i, z_3 = 1 - i, z_4 = \cdots = z_{(n-1)/2} = i$, and $z_{(n+1)/2} = \cdots = , z_n = 1$. If $A \ge (n+9)/2$, then we put m = A - (n-7)/2. Then we have $m \ge 8$, so there are z_1, \ldots, z_7 in Γ such that $z_1^2 + \cdots + z_7^2 = 0, N(z_1) + \cdots + N(z_7) = 2m, z_1 \neq 0, \ldots, z_7 \neq 0$ by the case n = 7. We put $z_8 = \cdots = z_{(n+7)/2} = 1$ and $z_{(n+9)/2} = i$. Thus the condition (\$) holds. \Box

LEMMA 3. Let m be a positive integer $\equiv \pm 1 \mod 5$. Then there are integers $a, b, c, d \in \mathbb{Z}$ such that

$$m = a^2 + 25(b^2 + c^2 + d^2), \quad ac \neq 0,$$

if and only if $m \notin G$, where G is the set defined by

$$G = \{19, 21, 31, 39, 49, 69, 71, 81, 119, 121, 179, 191, 211, 239, 379, 391\} \cup \{4^k, 9 \cdot 4^k, 11 \cdot 4^k, 6 \cdot 4^k, 14 \cdot 4^k, 46 \cdot 4^k, 94 \cdot 4^k : k \ge 0\}.$$

PROOF. Put $T = \{m = a^2 + 25(b^2 + c^2 + d^2) : a, b, c, d \in \mathbb{Z}, ac \neq 0, m \equiv \pm 1 \mod 5\}$. We note that if $m \equiv 0 \mod 8$, then $m \in T$ if and only if $m/4 \in T$. The necessity follows from direct calculations. Take a positive integer $m \notin G$ such that $m \not\equiv 0 \mod 8$ and $m \equiv \pm 1 \mod 5$. Then we can find an integer a such that $m \equiv a^2 \mod 25$ with $1 \leq a \leq 24$. We can assume that $m-a^2 \equiv 1, 2, 3, 5, 6 \mod 8$ (replacing a by 25-a if necessary). Thus, if $m > a^2$, then we have $(m - a^2)/25 = b^2 + c^2 + d^2$ with $c \neq 0$, which proves that $m \in T$ if $m > 24^2$. When $m < 24^2$, then we see that $m \in T$ by a direct calculation.

LEMMA 4. For a positive integer m, there are integers a, b, c, d, g in \mathbb{Z} such that

$$m = a^2 + b^2 + g^2(c^2 + d^2), \quad ac \neq 0, \quad g > 1, \quad g \quad odd,$$

if and only if $m \neq 5, 7, 9, 15, 21, 39, 4^k, 2 \cdot 4^k, 3 \cdot 4^k, 6 \cdot 4^k$

PROOF. We lose nothing by supposing $m \neq 0 \mod 8$. The necessity follows from a direct calculation. For the sufficiency, it suffices to show that m is of the desired form if $m \neq 0 \mod 8$ and $m \neq 1, 2, 3, 4, 5, 6, 7, 9, 12, 15, 21, 39$.

(1). Case $m \neq 0 \mod 3$. Putting c = 2 (if $m1 \mod 4$) or c = 1 (otherwise), we have $m - 9c^2 \neq 0, 4, 7 \mod 8$. This implies that $m - 9c^2 = a^2 + b^2 + d^2$ with $a, b, d \in \mathbb{Z}$ if $m > 9c^2$ (that is $m \neq 1, 2, 4, 5, 7, 13, 17, 25, 29$). We may assume that $d \equiv 0 \mod 3$, since $m \neq 0 \mod 3$. Thus we can write $m = a^2 + b^2 + 9(c^2 + d^2)$ with $ac \neq 0$, noticing that if a = b = 0 then we would have $m \equiv 0 \mod 3$. A direct calculation shows that it is true for m = 13, 17, 25, 29.

(2). Case $m \equiv 0 \mod 9$. If m > 9, then we can write $m/9 = a^2 + b^2 + c^2 + d^2$ with $ac \neq 0$, so $m = (3a)^2 + (3b)^2 + 9(c^2 + d^2)$.

(3). Case $m \equiv 0 \mod 3$ with $m \not\equiv 0 \mod 9$. Put m = 3h with $h \in \mathbb{Z}$ so $h \not\equiv 0 \mod 3$.

(i) If $h \equiv 0 \mod 25$, then m is of the desired form by a similar argument like the case $m \equiv 0 \mod 9$.

(ii) Suppose that $h \equiv 0 \mod 5$ with $h \not\equiv 0 \mod 25$. Putting $d_1 = 10$ (if $h \equiv 1 \mod 4$) or $d_1 = 5$ (otherwise), we have $h - d_1^2 \not\equiv 0, 4, 7 \mod 8$, which implies that $h - d_1^2 = a^2 + b^2 + c_1^2$ with $a, b, c_1 \in \mathbb{Z}$ if $h > d_1^2$ (that is $h \neq 10, 20, 65, 85$). The two integers $c = (3c_1 \pm 4d_1)/5$ and $d = (4c_1 \pm 3d_1)/5$ are prime to 5, taking a suitable sign. Hence we have $h = a^2 + b^2 + c^2 + d^2$ with $abcd \not\equiv 0 \mod 5$. This is also true for h = 10, 20, 65, 85. Now we may assume, since $h \equiv 0 \mod 5$, that $a \equiv d \equiv 1, b \equiv c \equiv 2 \mod 5$ by changing the signs if necessary. Putting

$$a_1 = b - c + d$$
, $b_1 = c - a + d$, $c_1 = a - b + d$, $d_1 = a + b + c$,

we have $m = 3h = a_1^2 + b_1^2 + c_1^2 + d_1^2$ with a_1

 $\equiv 1 \mod 5, c_1 \equiv d_1 \equiv 0 \mod 5$. If $c_1 = d_1 = 0$, then we would have $h = 3(a^2 + b^2)$, which is a contradiction. Hence *m* is of the desired form.

(iii) Suppose that $h \equiv \pm 1 \mod 5$. By Lemma 3, if $h \notin G$, then we have $h = a^2 + 25(b^2 + c^2 + d^2)$ with $ac \neq 0$. Using a similar argument

Y. MIMURA

as in (ii), we can write $25(b^2 + c^2) = b_1^2 + c_1^2$ with $b_1c_1 \not\equiv 0 \mod 5$. Hence we have $h = a^2 + b^2 + c^2 + 25d^2$ with $abc \not\equiv 0 \mod 5$. We may assume, since $h \equiv \pm 1 \mod 5$, that $a \equiv b \equiv 2c \mod 5$. Putting $a_1 = b - c + d, \ldots$ as in (ii), we have $m = 3h = a_1^2 + b_1^2 + c_1^2 + d_1^2$ with $a_1 \not\equiv 0$, $c_1 \equiv d_1 \equiv 0 \mod 5$. If $c_1 = d_1 = 0$ then we would have $h \equiv 0 \mod 3$. Thus m is of the desired form. If $h \in G$ with $h \neq 1, 4$, then we see that m is of the desired form by a direct calculation.

(iv) Suppose that $h \equiv \pm 2 \mod 5$. Then $m = 3h \equiv \pm 1 \mod 5$. By Lemma 3, if $h \notin G$, then we have $m = a^2 + (5b)^2 + 25(c^2 + d^2)$ with $ac \neq 0$. If $m \in G$, then m = 6, 21, 39, 69, since $m \equiv 0 \mod 3$. Notice that $69 = 2^2 + 4^2 + 49(1^2 + 0^2)$.

3. 3-frames. For 3-frames, we give the next theorem without a proof. But the problem is open for n = 5, 6.

THEOREM 5. Let $n \neq 5, 6$. Then E_n contains a proper 3-frame of scale A if and only if one of the following is satisfied:

- (1) n = 3, A is a square;
- (2) n = 4, A > 1;
- (3) $n \ge 7$, $n \equiv 1 \mod 3$, $A \ge (n+2)/3$;
- (4) $n \ge 8$, $n \equiv 2 \mod 3$, $A \ge (n+4)/3$;
- (5) $n \ge 9$, $n \equiv 0 \mod 3$, $A \ge n/3$.

DEPARTMENT OF MATHEMATICS, KOBE UNIVERSITY, ROKKO KOBE, JAPAN