Universal Positive Ternary Integral Quad. Forms over Real Quadratic Fields

Wai-kiu Chan
Dept. of Math., The Ohio State University, Columbus, OH 43210
Myung-Hwan Kim *
Dept. of Math., Seoul National University, Seoul 151-742, Korea
S. Raghavan
School of Math., SPIC Science Foundation, Madras 600017, India

Abstract

Maass [M] showed that the quadratic form $x^2+y^2+z^2$ is universal over the ring of integers of $\mathbf{Q}(\sqrt{5})$, i.e., it represents every totally positive integer in $\mathbf{Q}(\sqrt{5})$. In this paper, we extend this result to all real quadratic fields. We show that there are only three real quadratic fields which admit ternary universal classic integral quadratic forms; they are $\mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{3})$ and $\mathbf{Q}(\sqrt{5})$. In each of these fields, we determine all ternary universal classic integral quadratic forms.

Mathematics Subject Classification (1991) : 11E12, 11E20, 11E25
Short Running Title : Universal Quadratic Forms

November 1, 1994, Ohio State Univ., Columbus, Ohio, USA

*This work was done while the second author was visiting The Ohio State University. He acknowledges his gratitude to the university for its hospitality. He was partially supported by Seoam Foundation and Korean Ministry of Education (BSRIP-94-1414).

1 Introduction

In 1770, Lagrange proved the famous four square theorem. In the language of quadratic forms, it says that the form $x^2 + y^2 + z^2 + u^2$ represents all positive integers. At the beginning of this century, Ramanujan [R] extended Lagrange's result and he showed that up to equivalence, there are 54 diagonal positive quarternary integral quadratic forms which represent all positive integers. Later on, Dickson [D] further extended the results to non-diagonal cases.

In a totally real number field K, one may ask whether there exist positive integral quadratic forms over K which represent all totally positive integers in K. We call such quadratic forms universal. The results in the paper by Hsia, Kitaoka and Kneser [HKK] can easily imply that universal integral quadratic forms always exist. However, the quadratic forms constructed by their results may have too many variables. Therefore, one may want to find universal integral quadratic forms with fewest variables. It is easy to see that no positive binary quadratic forms can be universal. For the ternary case, Maass [M] showed that the sum of three squares is universal when $K = \mathbf{Q}(\sqrt{5})$. This cannot happen in any other K since Siegel [S1] proved that K admits a sum of squares that is universal if and only if $K = \mathbf{Q}$ or $\mathbf{Q}(\sqrt{5})$. However, K may admit other ternary universal integral quadratic forms and concerning this, Kitaoka conjectured in a private communication that there may be only finitely many K that admit such quadratic forms. In this paper, we confirm Kitaoka's conjecture for real quadratic fields K by characterizing those which admit classic ternary universal integral quadratic forms. An integral quadratic form is called classic if the coefficients of the crossed terms are divisible by 2, that is, the corresponding quadratic lattice is free and the scale is in the ring of integers of K. ¿From now on, by quadratic forms or simply by forms we will mean positive classic integral quadratic forms. In fact, we prove the following :

Theorem 1.1 *Let K be a real quadratic number field. Ternary universal quadratic forms over K exist if and only if $K = \mathbf{Q}(\sqrt{2})$, $\mathbf{Q}(\sqrt{3})$ or $\mathbf{Q}(\sqrt{5})$.*

We also determine all ternary universal quadratic forms over each of the above K's. They are, up to equivalence, as follows :

(1) Over $K = \mathbf{Q}(\sqrt{2})$:

$$x^2 + y^2 + (2+\sqrt{2})z^2, \quad x^2 + (2+\sqrt{2})y^2 + 2yz + (2-\sqrt{2})z^2,$$
$$x^2 + (2+\sqrt{2})y^2 + 2yz + 3z^2, \quad x^2 + (2-\sqrt{2})y^2 + 2yz + 3z^2.$$

(2) Over $K = \mathbf{Q}(\sqrt{3})$:

$$x^2 + y^2 + (2+\sqrt{3})z^2, \quad x^2 + (2+\sqrt{3})y^2 + (2+\sqrt{3})z^2.$$

(3) Over $K = \mathbf{Q}(\sqrt{5})$:

$$x^2 + y^2 + z^2, \quad x^2 + y^2 + 2z^2, \quad x^2 + y^2 + \frac{5+\sqrt{5}}{2}z^2,$$

$$x^2 + 2y^2 + 2yz + \frac{5+\sqrt{5}}{2}z^2, \quad x^2 + 2y^2 + 2yz + \frac{5-\sqrt{5}}{2}z^2.$$

We prove the necessity of Theorem 1.1 in Section 2 by showing that if $K = \mathbf{Q}(\sqrt{m})$ where m is a square free integer greater 5, then K does not admit any ternary universal form. In Sections 3, 4 and 5, we will prove (1), (2) and (3) above, from which the sufficiency of Theorem 1.1 also follows. There, we first show that the forms listed above are the only possible candidates for ternary universal forms. The universality of those forms are then proved by showing that they represent all totally positive integers locally everywhere and that they all have class number 1. An interesting observation from this is that all the universal forms over real quadratic fields are of class number 1.

Before we move on, we fix some notations. For any real quadratic number field K, let $\mathcal{O}$ be the ring of integers in K and $\mathcal{O}_+$ be the set of all totally positive integers. Let ϵ be the fundamental unit of K. For any two integers $\alpha, \beta \in \mathcal{O}$, we write $\alpha \sim \beta$ when $\alpha = \beta u^2$ for some unit $u \in \mathcal{O}$. The norm and trace from K to $\mathbf{Q}$ are denoted by N and Tr, respectively. For any element $\alpha \in \mathcal{O}$, α' will denote the conjugate of α.

In the following sections, we will adapt lattice theorectic languange. An $\mathcal{O}$-lattice means a finitely generated $\mathcal{O}$-module equipped with a bilinear form B. The corresponing quadratic map will be denoted by Q. Since classic integral quadratic forms correpond to free $\mathcal{O}$-lattices with scales contained in $\mathcal{O}$, we will assume every $\mathcal{O}$-lattice considered in this paper is such unless stated otherwise. For any unexplained terminologies and basic facts about quadratic lattices, we refer the readers to O'Meara's book [O1]. We conclude this section with a lemma which will be used frequently in this paper.

Lemma 1.1 *Let $\alpha, \gamma \in \mathcal{O}_+$, $\beta \in \mathcal{O}_+ \cup \{0\}$, and $x \in \mathcal{O}$ such that $\alpha x^2 + \beta = \gamma$. Then $0 \le \alpha x^2 \le \gamma$ and $0 \le (\alpha x^2)' \le \gamma'$ so that $0 \le N(\alpha x^2) \le N(\gamma)$. In particular, $N(\alpha) \le N(\gamma)$ if $x \ne 0$.*

Proof. Trivial. □

2 $m > 5$

In this section, we will prove the only if part of Theorem 1.1. Throughout this section, $K = \mathbf{Q}(\sqrt{m})$ where m is a square free integer greater than 5. We first give three propositions which are useful in future discussion.

Proposition 2.1 *(1)* $< 1 > \perp < 1 >$ *does not represent 3.*
(2) $< 1 > \perp < 1 >$ *does not represent* ϵ *if* $N(\epsilon) = 1$.
(3) $< 1 > \perp < \epsilon >$ *does not represent 2 if* $N(\epsilon) = 1$ *and* 2ϵ *is not a square.*
(4) $< 1 > \perp < \epsilon >$ *does not represent 5 if* $N(\epsilon) = 1$ *and* 2ϵ *is a square.*
(5) $< 1 > \perp < 2 >$ *does not represent 5.*

Proof. (1) - (5) follow immediately from the following observations. *Box*

$$(*) \begin{cases} \text{If } \alpha, 1-\alpha \in \mathcal{O}_+ \cup \{0\}, & \text{then } \alpha = 0 \text{ or } 1. \\ \text{If } \alpha, 2-\alpha \in \mathcal{O}_+ \cup \{0\}, & \text{then } \alpha = 0,\ 1 \text{ or } 2. \\ \text{If } \alpha, 3-\alpha \in \mathcal{O}_+ \cup \{0\}, & \text{then } \alpha = 0,\ 1,\ 2 \text{ or } 3. \\ \text{If } \alpha, 4-\alpha \in \mathcal{O}_+ \cup \{0\}, & \text{then } \alpha = 0,\ 1,\ 2,\ 3 \text{ or } 4. \\ \text{If } \alpha, 5-\alpha \in \mathcal{O}_+ \cup \{0\}, & \text{then } \alpha = 0,\ 1,\ 2,\ 3,\ 4,\ 5 \text{ or} \\ & 2 + \frac{1+\sqrt{m}}{2} \text{ for } m = 13,\ 17,\ 21. \end{cases}$$

We omit the proof of the following proposition since it is similar to that of Proposition 2.3 but is lengthier.

Proposition 2.2 *Let* α, β, γ *be positive rational integers. Then*
(1) $< \alpha > \perp < \beta > \perp < \gamma >$ *cannot represent* $\mu + \sqrt{m}$ *nor* $2\mu + 2\sqrt{m}$ *if* $m \equiv 2, 3$ *(mod 4) where* μ *is the smallest rational integer bigger than* $\sqrt{m}$.
(2) $< \alpha > \perp < \beta > \perp < \gamma >$ *cannot represent* $\frac{\nu+\sqrt{m}}{2}$ *nor* $\nu + \sqrt{m}$ *if* $m \equiv 1$ *(mod 4) where* ν *is the smallest rational odd integer bigger than* $\sqrt{m}$.

Proposition 2.3 *Suppose* $N(\epsilon) = 1$ *and* 2ϵ *is a square. If* γ *is a positive rational integer, then* $< 1 > \perp < \epsilon > \perp < \gamma >$ *cannot represent* $\mu + \sqrt{m}$ *where* μ *is the smallest rational integer bigger than* $\sqrt{m}$.

Proof. Observe that a necessary condition for 2ϵ being a square is that $m \equiv 2, 3 \pmod 4$. Suppose $x^2 + \epsilon y^2 + \gamma z^2 = \mu + \sqrt{m}$ for some $x, y, z \in \mathcal{O}$. Let $\epsilon y^2 = a + b\sqrt{m}$. Then it is clear that x and z are rational integers and hence $x^2 + a + \gamma z^2 = \mu$ and $b = 1$. Since $\epsilon y^2 \in \mathcal{O}_+$, we obtain $x = z = 0$ and $\epsilon y^2 = \mu + \sqrt{m}$. Now consider $2\epsilon y^2 = 2\mu + 2\sqrt{m}$. This is a square since 2ϵ is. So, $2\mu + 2\sqrt{m} = (c + d\sqrt{m})^2$ for some rational integers c and d. From

this, we get $c = d = \pm 1$ and $m + 1 = 2\mu < 2(\sqrt{m} + 1)$, which is not possible since $m > 5$. *Box*.

Let L be a tenary universal $\mathcal{O}$-lattice. Then L represents 1 and so $< 1 >$ splits L and hence $L \cong < 1 > \perp L_0$ for some binary sublattice L_0 of L. We have two cases : (I) L_0 represents a unit and (II) L_0 does not represent any unit.

Case (I) L_0 represents a unit.
It is clear that for some $\gamma \in \mathcal{O}_+$,

$$L \cong \begin{cases} < 1 > \perp < 1 > \perp < \gamma > & (a) \\ < 1 > \perp < \epsilon > \perp < \gamma > & (b) \end{cases}$$

where (b) occurs only if $N(\epsilon) = 1$. We treat (a) and (b) separately below.

(a) First assume $N(\epsilon) = -1$. By Proposition 2.1 (1), Lemma 1.1 and Siegel's result [S1], we have $2 \leq N(\gamma) \leq 9$. Using this and the equation $x^2 + y^2 + \gamma z^2 = 3$, one can show that $\gamma \sim 2$ or 3 and hence by Proposition 2.2, we can eliminate these two possibilities.

Now assume $N(\epsilon) = 1$. Then by Proposition 2.1 (2) and Lemma 1.1, we have $N(\gamma) = 1$ and hence by Siegel's result, $\gamma \sim \epsilon$ is the only possibility. We now claim that 2ϵ must be a square. Suppose not. Since 2ϵ is represented by L, there exist $x, y, z \in \mathcal{O}$ such that $\epsilon^{-1}x^2 + \epsilon^{-1}y^2 + z^2 = 2$. Then by $(*)$, $\epsilon^{-1}x^2 = 0$ because ϵ cannot be a square. Applying $(*)$ again to $\epsilon^{-1}y^2 + z^2 = 2$, we obtain $\epsilon^{-1}y^2 = 0$ and $z^2 = 2$, which is absurd. So 2ϵ is a square and hence the possibility $\gamma \sim \epsilon$ can be eliminated by Propostion 2.3. Therefore, we do not have any ternary universal $\mathcal{O}$-lattice in this case.

(b) By Proposition 2.1 (3),(4) and Lemma 1.1, we have

$$N(\gamma) \leq \begin{cases} 4 & \text{if } 2\epsilon \text{ is not a square} \\ 25 & \text{if } 2\epsilon \text{ is a square.} \end{cases}$$

Then applying $(*)$ repeatedly as above to the equations $x^2 + \epsilon y^2 + \gamma z^2 = 2$ or 5, respectively, one can show that

$$\gamma \sim \begin{cases} 1, 2 & \text{if } 2\epsilon \text{ is not a square} \\ 1, \epsilon, 2, 2\epsilon, 3, 4, 5 & \text{if } 2\epsilon \text{ is a square.} \end{cases}$$

The case $\gamma \sim 1$ is already ruled out in (a). Furthermore, by Proposition 2.3, we can reduce to

$$\gamma \sim \begin{cases} 2 & \text{if } 2\epsilon \text{ is not a square} \\ \epsilon, 2\epsilon & \text{if } 2\epsilon \text{ is a square.} \end{cases}$$

Assume 2ϵ is a square. The lattice $< 1 > \perp < \epsilon > \perp < \epsilon >$ cannot be universal because it can be obtained from scaling $< 1 > \perp < 1 > \perp < \epsilon >$ by ϵ. And neither can be $< 1 > \perp < \epsilon > \perp < 2\epsilon >$ because it is isometric to a sublattice of $< 1 > \perp < 1 > \perp < \epsilon >$. Now if 2ϵ is not a square, then the lattice $< 1 > \perp < \epsilon > \perp < 2 >$ cannot represent 2ϵ. The proof is almost same as that for the lattice $< 1 > \perp < 1 > \perp < \epsilon >$ and so we do not present it here.

Case (II) L_0 does not represent any unit.
In this case, we must have $N(\epsilon) = -1$. Since L represents 2, one can see immediately that L_0 must represent 2 also. For convenience, we divide this case into two subcases : (a) L_0 is diagonal and (b) L_0 is indecomposable.

(a) We may assume that $L_0 \cong < \beta > \perp < \gamma >$ for some $\beta, \gamma \in \mathcal{O}_+$. Since L_0 represents 2, there are $y, z \in \mathcal{O}$ such that $\beta y^2 + \gamma z^2 = 2$. We then have

$$N(\beta y^2) + Tr(\beta y^2 (\gamma z^2)') + N(\gamma z^2) = 4.$$

Since β and γ are not units, we can see that either $y = 0$ or $z = 0$. Without loss of generality, we may assume $z = 0$. Then $\beta y^2 = 2$. Since $N(\beta) \geq 2$, y^2 must be a unit and hence $\beta \sim 2$. Therefore $L_0 \cong < 2 > \perp < \gamma >$. By Proposition 2.1 (5) and Lemma 1.1, we have $N(\gamma) \leq 25$. Together with the equation $x^2 + 2y^2 + \gamma z^2 = 5$, we can show that $\gamma \sim 1, 2, \pi_2^2, (\pi_2')^2, 3, 4$ or 5, where π_2 is a prime element in $\mathcal{O}$ with $N(\pi_2) = 2$ when $2\mathbf{Z}$ splits into a product of two principal prime ideals. Proposition 2.2 rules out the cases $\gamma \sim 1, 2, 3, 4$ and 5. If $\gamma \sim \pi_2^2$ or $(\pi_2')^2$, then L is isometric to a sublattice of $< 1 > \perp < 2 > \perp < 1 >$ which is not universal again by Proposition 2.2. Therefore we do not have any universal ternary $\mathcal{O}$-lattice in this case.

(b) For any vector $\mathbf{v} \in L_0$, we use $\mathcal{I}_{\mathbf{v}}$ to denote the coefficient of $\mathbf{v}$. Take any $\mathbf{e} \in L_0$ such that $Q(\mathbf{e}) = 2$. Since $L_0/\mathcal{I}_{\mathbf{e}}\mathbf{e}$ is finitely generated and torsion free, it is projective (see [J]) and so we can find a vector $\mathbf{f} \in L_0$ such that $L_0 = \mathcal{I}_{\mathbf{e}}\mathbf{e} + \mathcal{I}_{\mathbf{f}}\mathbf{f}$. Since $Q(\mathbf{e}) = 2$, $\mathcal{I}_{\mathbf{e}}$ can be $\mathcal{O}$ or $\wp^{-1}$ where $\wp$ is the unique dyadic prime of $\mathcal{O}$ when $2\mathbf{Z}$ ramifies. We treat these two cases separately.

Firstly, let $\mathcal{I}_{\mathbf{e}} = \mathcal{O}$. Then $\mathcal{I}_{\mathbf{f}} = \mathcal{O}$ because L_0 is free. Therefore

$$L_0 = \mathcal{O}\mathbf{e} + \mathcal{O}\mathbf{f} \cong \left\langle \begin{array}{cc} 2 & \beta \\ \beta & \gamma \end{array} \right\rangle$$

where $B(\mathbf{e}, \mathbf{f}) = \beta \in \mathcal{O}$ and $Q(\mathbf{f}) = \gamma \in \mathcal{O}_+$. Note that $\beta \notin 2\mathcal{O}$ because otherwise $\mathcal{O}\mathbf{e}$ splits L_0 and it contradicts to the hypothesis that L_0 is indecomposable. Since L represents 5, L_0 represents 4 or 5. So, there exist

$y, z \in \mathcal{O}$ such that $2y^2 + 2\beta yz + \gamma z^2 = 4$ or 5. By completing square and multiplying 2, we have $(2y + \gamma z)^2 + (2\gamma - \beta^2)z^2 = 8$ or 10.

If $m \equiv 2, 3 \pmod 4$, then the smallest m with $N(\epsilon) = -1$ is 10. So we may assume $m \geq 10$ here. It is easy to see that $(2y+\beta z)^2$ must be a rational integer square and hence $(2\gamma - \beta^2)z^2 = 1, 4, 6, 7, 8, 9$ or 10. From this, one can show that $2\gamma - \beta^2 = 1, 2, \pi_3^2, (\pi_3')^2, 4, 6, 7, 8, 9$ or 10 by adjusting the vector $\mathbf{f}$ suitably. The element π_3 is a prime element in $\mathcal{O}$ with $N(\pi_3) = 3$ when $3\mathbf{Z}$ splits into a product of two distinct principal prime ideals. Now, since L is universal, the lattice $< 2 > \perp < 1 > \perp < 2\gamma - \beta^2 >$ should represent all integers in $2\mathcal{O}_+$ which is impossible in view of Proposition 2.2 (1) if $2\gamma - \beta^2 \in \mathbf{Z}$. Therefore $2\gamma - \beta^2$ can only be π_3^2 or $(\pi_3')^2$. However, these are also impossible because otherwise $< 2 > \perp < 1 > \perp < 1 >$ represents $2\mu + 2\sqrt{m}$ which is absurd again by Proposition 2.2 (1).

Suppose $m \equiv 1 \pmod 4$. The smallest m with $N(\epsilon) = -1$ is 13. So we may assume $m \geq 13$. If $m > 40$, we may argue as in previous paragraph to obtain $2\gamma - \beta^2 = 1, \pi_2^2, (\pi_2')^2, \pi_3^2, (\pi_3')^2, 4, 6, 7, 8, 9$ or 10. Since L is universal, $< 2 > \perp < 1 > \perp < 2\gamma - \beta^2 >$ represents $\nu + \sqrt{m} \in 2\mathcal{O}$ which is impossible by Proposition 2.2 (2) if $2\gamma - \beta^2 \in \mathbf{Z}$. The remaining cases are also impossible because they would imply that $< 2 > \perp < 1 > \perp < 1 >$ represents $\nu + \sqrt{m}$. When $m \leq 40$, the only possible m's are 13, 17, 29 and 37. Again we consider the equation $(2y + \beta z)^2 + (2\gamma - \beta^2)z^2 = 8$ or 10. Although the first term may no longer be a rational integer square, one can directly check that when $m = 29$ and 37, we have the same candidates as above and they can be ruled out by Proposition 2.2 (2). When $m = 13$ and 17, beside the candidates listed above, which can be eliminated again by Proposition 2.2 (2), we have eight additional candidates : $2\gamma - \beta^2 = \frac{9 \pm \sqrt{13}}{2}$ or $\frac{13 \pm \sqrt{13}}{2}$ when $m = 13$; $2\gamma - \beta^2 = \frac{7 \pm \sqrt{17}}{2}$ or $\frac{11 \pm \sqrt{17}}{2}$ when $m = 17$. However, none of these are possible since L cannot represent $\frac{5+\sqrt{13}}{2}$ when $2\gamma - \beta^2 = \frac{9 \pm \sqrt{13}}{2}$ or $\frac{13 \pm \sqrt{13}}{2}$; $\frac{5+\sqrt{17}}{2}$ when $2\gamma - \beta^2 = \frac{7 \pm \sqrt{7}}{2}$ or $\frac{11 \pm \sqrt{17}}{2}$.

Secondly, let $\mathcal{I}_{\mathbf{e}} = \wp^{-1}$. This case happens only when $m \equiv 2, 3 \pmod 4$. Recall that $N(\epsilon) = -1$. The lattice L_0 can be written as $\wp^{-1}\mathbf{e} + \wp\mathbf{f}$. Let $B(\mathbf{e}, \mathbf{f}) = \beta \in \mathcal{O}$ and $Q(\mathbf{f}) = \gamma \in \mathcal{O}_+$. Again, from the representation of 4 or 5 by L_0, we obtain $(2y + \beta z)^2 + (2\gamma - \beta^2)z^2 = 8$ or 10. where $y \in \wp^{-1}$ and $z \in \wp$. Since $2y \in \mathcal{O}$, $(2y + \beta z)^2$ is still in $\mathcal{O}$. Therefore, $(2y + \beta z)^2$ is again a square of a rational integer and this gives $(2\gamma - \beta^2)z^2 = 4, 6, 8$ or 10 since $z \in \wp$. ¿From these, one can show that $2\gamma - \beta^2 = 1$ or 2 by adjusting $\mathbf{f}$ suitably. By a similar argument using Proposition 2.2 (1) as above, one can eliminate these possibilities, too.

In conclusion, we have shown that if $K = \mathbf{Q}(\sqrt{m})$ with $m > 5$ and square-free, then K does not admit any ternary universal quadratic forms.

3 $m = 2$

In this section, we will determine all ternary universal $\mathcal{O}$-lattices over the field $\mathbf{Q}(\sqrt{2})$. Note that $\epsilon = 1 + \sqrt{2}$ and $N(\epsilon) = -1$. We need the following proposition but we omit the proof since it is straightforward.

Proposition 3.1 *Let $L \cong < 1 > \perp < 1 + \epsilon > \perp < \gamma >$ be a positive $\mathcal{O}$-lattice. Then L cannot represent $3 + 3\epsilon$ if $\gamma = 2$ or 3.*

Let L be a ternary universal $\mathcal{O}$-lattice. As before, $L \cong < 1 > \perp L_0$ for some binary $\mathcal{O}$-lattice. If L_0 represents a unit, then L_0 represents 1 and so $L \cong < 1 > \perp < 1 > \perp < \gamma >$. It can be checked that $< 1 > \perp < 1 >$ does not represent $1+\epsilon \in \mathcal{O}_+$. Therefore, by Lemma 1.1, we have $N(\gamma) \leq N(1+\epsilon) = 2$ and so $\gamma \sim 1$ or $1 + \epsilon$. Since $< 1 > \perp < 1 > \perp < 1 >$ is not universal by [S1], we just have one candidate in this case :

$$W = < 1 > \perp < 1 > \perp < 1 + \epsilon > .$$

If L_0 does not represent any unit, then L_0 must represent $1 + \epsilon$. We divide this case into two subcases :

(a) L_0 is diagonal : Since $1 + \epsilon$ cannot be a sum of totally positive integers, $< 1 + \epsilon >$ should split L_0. So, $L \cong < 1 > \perp < 1 + \epsilon > \perp < \gamma >$ with $N(\gamma) \geq 2$. Now applying $(*)$ to $x^2 + (1 + \epsilon)y^2 + \gamma z^2 = 3$, we obtain $\gamma \sim 2, 3$. By Proposition 3.1, however, neither can make L universal.

(b) L_0 is indecomposable : Take any vector $\mathbf{e} \in L_0$ such that $Q(\mathbf{e}) = 1 + \epsilon$. Clearly, $\mathbf{e}$ is a maximal vector in L_0. So, $L_0 = \mathcal{O}\mathbf{e} + \mathcal{O}\mathbf{f}$ for some $\mathbf{f} \in L_0$. Let $B(\mathbf{e}, \mathbf{f}) = \beta \in \mathcal{O}$ and $Q(\mathbf{f}) = \gamma \in \mathcal{O}_+$. If $\beta \in \wp = (1 + \epsilon)\mathcal{O}$, then $\mathcal{O}\mathbf{e}$ splits L_0 which is impossible. Therefore, $\beta \notin \wp$. Since $|\mathcal{O}/\wp| = N\wp = 2$, we may assume $\beta = 1$ by adjusting $\mathbf{f}$ suitably. The following proposition says that the discriminant of L determines the isometry class of L.

Proposition 3.2 *If the discriminant of $L_0 \cong \left\langle \begin{matrix} 1+\epsilon & 1 \\ 1 & \gamma_0 \end{matrix} \right\rangle$ and $L_1 \cong \left\langle \begin{matrix} 1+\epsilon & 1 \\ 1 & \gamma_1 \end{matrix} \right\rangle$ are the same, then they are isometric.*

Proof. Suppose $(1+\epsilon)\gamma_1 - 1 = ((1+\epsilon)\gamma_0 - 1)\epsilon^{2n}$. Cleary $1-\epsilon^{2n}$ is divisible by $1+\epsilon$. Therefore either $1+\epsilon^n$ or $1-\epsilon^n$ is divisble by $1+\epsilon$. However, $(1+\epsilon^n)+(1-\epsilon^n) = 2$ is divisible by $1+\epsilon$. Therefore both $1+\epsilon^n$ and $1-\epsilon^n$ must be divisible by $1+\epsilon$. Let $\{\mathbf{e}_i, \mathbf{f}_i\}$ be a basis of L_i such that $Q(\mathbf{e}_i) = 1+\epsilon$, $B(\mathbf{e}_i, \mathbf{f}_i) = 1$ and $Q(\mathbf{f}_i) = \gamma_i$ for $i = 0, 1$. Now it is direct to check that the linear map $\sigma : L_0 \longrightarrow L_1$ defined by $\mathbf{e}_0 \longmapsto \mathbf{e}_1$, $\mathbf{f}_0 \longmapsto \frac{1-\epsilon^{-n}}{1+\epsilon}\mathbf{e}_1 + \epsilon^{-n}\mathbf{f}_1$ is an isometry. *Box*

Since L represents 3, L_0 should represent 2 or 3. If L_0 represents 2, then there exist $y, z \in \mathcal{O}$ such that $(1+\epsilon)y^2+2yz+\gamma z^2 = 2$. By completing square and multiplying $1+\epsilon$, we obtain $((1+\epsilon)y+z)^2 + ((1+\epsilon)\gamma - 1)z^2 = 2+2\epsilon$. By norm consideration, we can see that $(1+\epsilon)\gamma - 1 \sim 1$. By Proposition 3.2, we can simply choose $\gamma = 1+\epsilon'$. If L_0 represent 3, by a similar argument, we obtain $\gamma = 3$ or $3+6\epsilon'$. Observing

$$\left\langle \begin{array}{cc} 1+\epsilon & 1 \\ 1 & 3+6\epsilon' \end{array} \right\rangle \cong \left\langle \begin{array}{cc} 1+\epsilon' & 1 \\ 1 & 3 \end{array} \right\rangle,$$

we obtain three more candidates :

$$M =< 1 > \perp \left\langle \begin{array}{cc} 1+\epsilon & 1 \\ 1 & 1+\epsilon' \end{array} \right\rangle,$$

$$J =< 1 > \perp \left\langle \begin{array}{cc} 1+\epsilon & 1 \\ 1 & 3 \end{array} \right\rangle, \quad J' =< 1 > \perp \left\langle \begin{array}{cc} 1+\epsilon' & 1 \\ 1 & 3 \end{array} \right\rangle.$$

Theorem 3.1 *Let $K = \mathbf{Q}(\sqrt{2})$. Up to isometry, the lattices W, M, J and J' are the only ternary universal $\mathcal{O}$-lattices.*

Proof. It suffices to show that W, M, J are universal since J' is conjugate to J. To accomplish this, we prove

(A) Each of them represents all totally positive integers locally everywhere.
(B) They all have class number 1.

Proof of (A) :
At the nondyadic primes $\wp$: The localization $W_\wp$ and $M_\wp$ are unimodular. So they represent all integers in $\mathcal{O}_\wp$ [O1, 92:1]. For $J_\wp$, it is unimodular at all other primes except at $\wp = \pi_7\mathcal{O}$, where $\pi_7 = 2+3\epsilon$. At this $\wp$, $J_\wp \cong < 1 > \perp < 1+\epsilon > \perp < (1+\epsilon)\pi_7 >$. Since $-(1+\epsilon) \equiv \epsilon^2 \pmod{\pi_7}$, $< 1 > \perp < 1+\epsilon >$ is hyperbolic and hence $J_\wp$ represents all integers at this $\wp$ also.

At the dyadic prime $\wp = (1+\epsilon)\mathcal{O}$: The lattices $J_\wp$ and $M_\wp$ are unimodular at $\wp$. It is easy to see that their norm groups are $\mathcal{O}_\wp^2 + \wp$ which is just $\mathcal{O}_\wp$. By Riehm's theorem [Ri, Theorem 7.4], $Q(J_\wp)$ and $Q(M_\wp)$ contain precisely the elements in their respective norm groups which are represented by the ambient spaces. But since $K_\wp J_\wp$ and $K_\wp M_\wp$ are isotropic, $Q(J_\wp) = Q(M_\wp) = \mathcal{O}_\wp$.

For $W_\wp$, it is not unimodular so Riehm's theorem cannot apply. However, one can check directly that $W_\wp$ represents all the square classes of $\mathcal{O}_\wp$.

At the infinite primes : Clearly, $W_\wp, M_\wp$ and $J_\wp$ represent all positive real numbers.

Proof of (B) :
For any positive $\mathcal{O}$-lattice L, the mass of L is defined to be

$$m(L) = \sum_{L_i} \frac{1}{|O(L_i)|}$$

where L_i runs through a complete set of representatives of classes in the genus of L and $|O(L_i)|$ is the order of the orthogonal group of L_i. If we can show that $m(L)$ is equal to $\frac{1}{|O(L)|}$, then L must have class number 1. Siegel [S2] proved that $m(L)$ can be expressed as an infinite product of local densities. Körner [K] provided formulae of the local densities for binary and ternary $\mathcal{O}$-lattices over real quadratic fields (see Satz 4, 6 and Hilfssatz 26 in his paper). It is then a direct application of Körner's results to show that $m(W) = \frac{1}{16}, m(M) = \frac{1}{32}$ and $m(J) = \frac{1}{8}$. On the other hand, from a simple computation, we obtain $|O(W)| = 16, |O(M)| = 32$ and $|O(J)| = 8$. So, the class numbers of M, W and J are all 1. *Box*

4 $m = 3$

In this section $K = \mathbf{Q}(\sqrt{3}), \epsilon = 2 + \sqrt{3}$ and $N(\epsilon) = 1$. Let L be a ternary universal $\mathcal{O}$-lattice. Then $L \cong < 1 > \perp < \epsilon > \perp < \gamma >$. It is easy to see that $< 1 > \perp < \epsilon >$ cannot represent $2 + \epsilon$. By Lemma 1.1, we have $N(\gamma) \leq N(2+\epsilon) = 13$. Therefore, $\gamma \sim 1, \epsilon, 2, 1+\epsilon, 1+\epsilon', 3, 2+\epsilon$ or $2+\epsilon'$. One can check that

$$L \quad \text{cannot represent} \begin{cases} 1+2\epsilon & \text{if } \gamma = 2, 3 \\ 3+2\epsilon & \text{if } \gamma = 1+\epsilon, 1+\epsilon' \\ 5+2\epsilon & \text{if } \gamma = 2+\epsilon, 2+\epsilon'. \end{cases}$$

Therefore we have only two candidates remaining in these cases :

$$E =< 1 >\perp< 1 >\perp< \epsilon >, \quad E^{\epsilon} =< 1 >\perp< \epsilon >\perp< \epsilon > .$$

Theorem 4.1 *Let $K = \mathbf{Q}(\sqrt{3})$. Up to isometry, E and E^{ϵ} are the only ternary universal $\mathcal{O}$-lattices.*

It suffices to show the universality for E. We omit the proof since it is similar to that of Theorem 3.1. As a remark, we record that $m(E) = \frac{1}{16}$ and $|O(E)| = 16$.

5 $m = 5$

In this section, $K = \mathbf{Q}(\sqrt{5}), \epsilon = \frac{1+\sqrt{5}}{2}$ and $N(\epsilon) = -1$. Let L be a ternary universal $\mathcal{O}$-lattice. As before, $L \cong < 1 >\perp L_0$ for some binary $\mathcal{O}$-lattice L_0. We need the following proposition.

Proposition 5.1 *Let γ be a totally positive integer. Then*
(1) $< 1 >\perp< 1 >\perp< \gamma >$ is not universal if $\gamma = 3, 3+\epsilon$ or $3+\epsilon'$.
(2) $< 1 >\perp< 2 >\perp< \gamma >$ is not universal if $\gamma = 2$ or $2+\epsilon$.

Proof. We just provide totally positive integers that are not represented by the lattice. (1) $< 1 >\perp< 1 >\perp< \gamma >$ cannot represent $3+\epsilon$ if $\gamma = 3$; $7+\epsilon'$ if $\gamma = 3+\epsilon$; $7+\epsilon$ if $\gamma = 3+\epsilon'$. (2) $< 1 >\perp< 2 >\perp< \gamma >$ cannot represent $2+\epsilon$ if $\gamma = 2$; $4+2\epsilon$ if $\gamma = 2+\epsilon$. *Box*

If L_0 represents a unit, then $L \cong < 1 >\perp< 1 >\perp< \gamma >$. Since $3+\epsilon$ cannot be represented by $< 1 >\perp< 1 >$, we have $N(\gamma) \leq N(3+\epsilon) = 11$. Therefore $\gamma \sim 1, 2, 2+\epsilon, 3, 3+\epsilon$ or $3+\epsilon'$. Proposition 5.1 (1) then leaves us the following candidates :

$$I =< 1 >\perp< 1 >\perp< 1 >, \quad S =< 1 >\perp< 1 >\perp< 2 >,$$

$$T =< 1 >\perp< 1 >\perp< 2+\epsilon > .$$

The lattice I corresponds to Masses's three square theorem.

If L_0 does not represent any unit, then L_0 must represent 2. Any vector of length 2 is a maximal vector in L_0. As in Section 3, we divide the dicussion into two cases.

(a) L_0 is diagonal : In this case, $L \cong < 1 >\perp< 2 >\perp< \gamma >$. Since $2+\epsilon$ cannot be represented by $< 1 >\perp< 2 >$, we have $2 \leq N(\gamma) \leq N(2+\epsilon) = 5$.

So, $\gamma \sim 2$ or $2+\epsilon$. However, neither can make L universal by Proposition 5.1 (2).

(b) L_0 is indecomposable : Since $\{0, 1, \epsilon, \epsilon'\}$ is a complete set of representatives of $\mathcal{O}/2\mathcal{O}$, we can assume that $L \cong < 1 > \perp \left\langle \begin{array}{cc} 2 & 1 \\ 1 & \gamma \end{array} \right\rangle$ by a similar argument as in Section 3 (b). We omit the proof the following propositon since it is almost identical to that of Proposition 3.2.

Proposition 5.2 *If the discriminants of* $\left\langle \begin{array}{cc} 2 & 1 \\ 1 & \gamma_0 \end{array} \right\rangle$ *and* $\left\langle \begin{array}{cc} 2 & 1 \\ 1 & \gamma_1 \end{array} \right\rangle$ *are the same, then they are isometric.*

One can proceed as in Section 3 to obtain $2\gamma - 1 \sim 5 - 2\epsilon$ or $3 + 2\epsilon$ from the representation of $2+\epsilon$ by L. By Proposition 5.2, we may assume $\gamma = 2 + \epsilon'$ or $2 + \epsilon$. Therefore we have two more candidates :

$$R = < 1 > \perp \left\langle \begin{array}{cc} 2 & 1 \\ 1 & 2+\epsilon \end{array} \right\rangle, \quad R' = < 1 > \perp \left\langle \begin{array}{cc} 2 & 1 \\ 1 & 2+\epsilon' \end{array} \right\rangle.$$

Now the following theorem can be proved similarly as in Theorem 3.1.

Theorem 5.1 *Let* $K = \mathbf{Q}(\sqrt{5})$. *Up to isometry,* I, S, T, R *and* R' *are the only ternary universal* $\mathcal{O}$*-lattices.*

As a remark, we record that $m(I) = \frac{1}{48}, m(S) = m(T) = \frac{1}{16}$ and $m(R) = \frac{1}{8}$ while $|O(I)| = 48, |O(S)| = |O(T)| = 16$, and $|O(R)| = 8$.

References

[D] L.E. Dickson, 'Quaternary Quadratic Forms Representing All Integers', *Amer. J. Math.* 49 (1927), 39-56.

[HKK] J.S. Hsia, Y. Kitaoka, M. Kneser, 'Representation of positive definite quadratic forms', *J. reine angew. Math.* 301 (1978), 132-141.

[J] N. Jacobson, *Basic Algebra II*, W.H. Freeman and Company, 1980.

[K] O. Körner, 'Die Maβe der Geschlechter quadratischer Formen vom Range ≤ 3 in quadratischen Zahlkörpern', *Math. Ann.*, 193 (1971), 279-314.

[M] H. Maass, 'Über die Darstellung total positiver Zahlen des Körpers $R(\sqrt{5})$ als Summe von drei Quadraten', *Abh. Math. Sem. Hamburg* 14 (1941), 185-191.

[O1] O.T. O'Meara, *Introduction to Quadratic Forms*, Springer Verlag, 1973.

[O2] O.T. O'Meara, 'The Integral Representation of Quadratic Forms over Local Fields', *Amer. J. Math.* 80 (1958), 843-878.

[R] S. Ramanujan, 'On the Expression of a Number in the Form $ax^2 + by^2 + cz^2 + du^2$', *Proc. Cambridge Phil. Soc.* 19 (1917), 11-21.

[Ri] C. Riehm, 'On the Integral Representations of Quadratic Forms over Local Fields', *Amer. J. Math.* 86 (1964), 25-62.

[S1] C.L. Siegel, 'Sums of mth Powers of Algebraic Integers', *Ann. Math.* 46 (1945), 313-339.

[S2] C.L. Siegel, 'Über die Analytische Theorie der quadratischen Formen I, II, III', *Ann. Math.* 36 (1935), 527-606; *ibid.* 37 (1936), 230-263; *ibid.* 38 (1937), 212-291.