*Journal de Théorie des Nombres*
*de Bordeaux* **12** (2000), 147–164

# On integral representations by totally positive ternary quadratic forms

par Elise BJÖRKHOLDT

Résumé. Soit $K$ un corps de nombres algébrique totalement réel dont l'anneau d'entiers $R$ est un anneau principal. Soit $f(x_1, x_2, x_3)$ une forme quadratique ternaire totalement définie à coefficients dans $R$. Nous étudions les représentations par $f$ d'entiers totalement positifs $N \in R$. Nous démontrons une formule qui lie le nombre de représentations de $N$ par des classes différentes dans le genre de $f$, au nombre de classes de $R[\sqrt{-c_f N}]$, où $c_f \in R$ est une constante qui dépend seulement de $f$. Nous donnons une démonstration algébrique du résultat classique de H. Maass sur les représentations comme sommes de trois carrés d'entiers de $\mathbb{Q}(\sqrt{5})$ et une dépendance explicite entre le nombre de représentations et le nombre de classes du corps biquadratique correspondant. Nous donnons également des formules analogues pour certaines formes quadratiques provenant d'ordres quaternioniques maximaux de nombre de classe 1, sur les entiers de corps de nombres quadratiques réels.

Abstract. Let $K$ be a totally real algebraic number field whose ring of integers $R$ is a principal ideal domain. Let $f(x_1, x_2, x_3)$ be a totally definite ternary quadratic form with coefficients in $R$. We shall study representations of totally positive elements $N \in R$ by $f$. We prove a quantitative formula relating the number of representations of $N$ by different classes in the genus of $f$ to the class number of $R[\sqrt{-c_f N}]$, where $c_f \in R$ is a constant depending only on $f$. We give an algebraic proof of a classical result of H. Maass on representations by sums of three squares over the integers in $\mathbb{Q}(\sqrt{5})$ and obtain an explicit dependence between the number of representations and the class number of the corresponding biquadratic field. We also give similar formulae for some quadratic forms arising from maximal quaternion orders, with class number one, over the integers in real quadratic number fields.

Manuscrit reçu le 18 juin 1999.

## Introduction

Let $f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$ and let $N \in \mathbb{Z}$ be a square-free positive integer such that $N \neq 1, 3$. Let $S = \mathbb{Z}[\sqrt{-N}]$. Gauss proved that the number of solutions $(x_1, x_2, x_3) \in \mathbb{Z}^3$ to the equation $f(x_1, x_2, x_3) = N$ is

$$r_f(N) = \begin{cases} 12h(S) & \text{for } N \equiv 1, 2 \pmod 4, \\ 8h(S) & \text{for } N \equiv 3 \pmod 8, \\ 0 & \text{for } N \equiv 7 \pmod 8, \end{cases}$$

where $h(S)$ denotes the class number of $S$.

In 1940 it was shown by Maass, using analytical means, that the equation $f(x_1, x_2, x_3) = N$ can be solved in $R = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ for every totally positive $N \in R$. Maass also gave a formula for the number of solutions (see [12]). In the present article, using algebraic methods and some numerical computations, we prove an explicit formula stating that the number of primitive representations $r_f^0(N)$ of a totally positive non-unit $N \in R$ (that is, solutions to $f(x_1, x_2, x_3) = N$ such that $GCD(x_1, x_2, x_3) = 1$) is given by

$$r_f^0(N) = \gamma_i h(S),$$

where $S = R[\sqrt{-N}]$ and $\gamma_i = 12, 24$ or $32$ (see Thm. 4.2). Moreover, we prove that there is always a primitive representation of $N$ by $f$. Using similar methods, we also discuss some other results on representations of integers by totally definite ternary quadratic forms with integer coefficients in totally real algebraic number fields.

Similar algebraic methods in connection with studies of representations by sums of three squares and some other ternary quadratic forms are already known from several papers (see [2], [4], [5], [15], [17], [18]). Following [2] and [4], where these questions were considered in the case of rational integers, we describe a strategy, which can be used for totally definite ternary quadratic forms over the integers in totally real algebraic number fields.

Let $R$ be a principal ideal domain whose quotient field $K$ is a totally real algebraic number field. Let $f(x_1, x_2, x_3)$ be a totally definite ternary quadratic form over $R$ and let $N \in R$ denote a totally positive number. In Section 1, we introduce some notation used in the paper. Section 2 contains a quantitative formula relating the number of representations of $N$ by different classes in the genus of $f$ to the class number of $S = R[\sqrt{-c_f N}]$, where $c_f \in R$ is a totally positive constant, which only depends on $f$. In the case of primitive representations, the right hand side of the formula is a product of the class number of $S$ by a coefficient $\gamma(N)$. The results of this section are direct generalizations of the results in [2] from the case of rational integers to the class number one case of the integers in totally real algebraic number fields. Therefore, we only modify some statements, and their proofs when necessary. In Section 3, we examine the stability for the embedding numbers of commutative quadratic orders into some quaternion orders. As a consequence we show that $\gamma(N)$ has a certain kind of periodicity. Finally, in Sections 4 and 5, we consider applications of our results obtaining a number of quantitative formulae for numbers of integral representations by specific ternary quadratic forms.

I would like to express my thanks to Juliusz Brzezinski for many valuable comments on this paper.

## 1. Preliminaries

Throughout this article, $R$ will denote a principal ideal domain whose quotient field $K$ is a totally real algebraic number field and $f : R^3 \to R$ will be a totally positive definite quadratic form. We denote by $N \gg 0$ that $N$ is totally positive. We let $\hat{R}_{\mathfrak{p}}$ denote the completion of $R$ with respect to a non-zero prime ideal $\mathfrak{p} \subset R$. $A$ will denote a quaternion algebra over $K$ i.e. a central simple $K$-algebra of dimension four.

An $R$-order $\Lambda$ is a subring of $A$ containing $R$, finitely generated and projective as an $R$-module and such that $K\Lambda = A$. We let $\hat{\Lambda}_{\mathfrak{p}} = \hat{R}_{\mathfrak{p}} \otimes_R \Lambda$ denote the completion of $\Lambda$ at $\mathfrak{p}$. Two $R$-orders $\Lambda$ and $\Lambda^{'}$ in $A$ are in the same genus if $\hat{\Lambda}_{\mathfrak{p}}$ and $\hat{\Lambda}^{'}_{\mathfrak{p}}$ are $\hat{R}_{\mathfrak{p}}$-isomorphic for each prime ideal $\mathfrak{p} \neq 0$ in $R$.

If $L$ is a free $R$-lattice with basis $e_1, e_2, e_3$ and $q$ is a quadratic form,

$$q : L \to R, \quad q(x_1e_1 + x_2e_2 + x_3e_3) = \sum_{1 \le i \le j \le 3} a_{ij}x_ix_j,$$

then the Clifford algebra, which we denote by $C(L, q)$ or $C(q)$, is $\mathcal{T}(L)/\mathcal{I}$ where $\mathcal{T}(L)$ is the tensor algebra of $L$ and $\mathcal{I}$ is the ideal in $\mathcal{T}(L)$ generated by $x \otimes x - q(x)$ for $x \in L$. The even Clifford algebra is defined to be

$$C_0(L, q) = \mathcal{T}_0(L)/\mathcal{I},$$

where $\mathcal{T}_0(L) = \bigoplus \mathcal{T}^{\otimes 2r}(L)$ is the even part of the tensor algebra of $L$.

Let $f(x_1, x_2, x_3) = \sum_{1 \le i \le j \le 3} a_{ij}x_ix_j = q(x_1e_1 + x_2e_2 + x_3e_3)$. The matrix

$$M_f = \begin{pmatrix} 2a_{11} & a_{12} & a_{13} \\ a_{12} & 2a_{22} & a_{23} \\ a_{13} & a_{23} & 2a_{33} \end{pmatrix}$$

is called the matrix of $f$ and $d(f) = \frac{1}{2}\det M_f$ is called the discriminant of $f$. We denote by $\Omega_f$ the greatest common divisor of the elements in the adjoint matrix of $M_f$. With $q$ non-degenerate, $C_0(L, q) \otimes_R K$ is a quaternion $K$-algebra. Furthermore, the square-root of the discriminant of the $R$-order $\Lambda = C_0(L, q)$, called the reduced discriminant and denoted by $d(\Lambda)$, has $d_\Lambda = \frac{1}{2}\det M_f$ as a generator (see [14], Satz 7).

Recall that an $R$-order $\Lambda$ is called hereditary if every ideal of $\Lambda$ is projective as a $\Lambda$-module and this occurs if and only if its discriminant $d_\Lambda$ is square-free (see [16], Prop. 39.14). $\Lambda$ is called Gorenstein if its dual $\Lambda^\# = \{x \in A : tr_{A/K}(x\Lambda) \subseteq R\}$ is projective as a left $\Lambda$-module ($tr_{A/K}$ denotes the trace function). $\Lambda$ is called a Bass order if each $R$-order $\Lambda'$ such that $\Lambda \subseteq \Lambda' \subseteq A$ is Gorenstein. For a quaternion order $\Lambda$ there is a Gorenstein order $G(\Lambda)$ containing $\Lambda$ such that $\Lambda = R + b(\Lambda)G(\Lambda)$, where $b(\Lambda)$ is an $R$-ideal. $G(\Lambda)$ and $b(\Lambda)$ are unique (see [3], p. 167).

We also recall that for an $R$-order $\Lambda$ in a quaternion algebra over $K$ the Eichler symbol, denoted by $e_\mathfrak{p}(\Lambda)$, is defined according to the following:

$$e_\mathfrak{p}(\Lambda) = \begin{cases} -1 & \text{if } \hat{\Lambda}_\mathfrak{p}/J(\hat{\Lambda}_\mathfrak{p}) \text{ is a quadratic field extension of } \hat{R}_\mathfrak{p}/\mathfrak{m}, \\ 0 & \text{if } \hat{\Lambda}_\mathfrak{p}/J(\hat{\Lambda}_\mathfrak{p}) \cong \hat{R}_\mathfrak{p}/\mathfrak{m}, \\ 1 & \text{if } \hat{\Lambda}_\mathfrak{p}/J(\hat{\Lambda}_\mathfrak{p}) \cong \hat{R}_\mathfrak{p}/\mathfrak{m} \times \hat{R}_\mathfrak{p}/\mathfrak{m}, \end{cases}$$

where $J(\Lambda)$ denotes the Jacobson radical of $\Lambda$ and $\mathfrak{m}$ denotes the maximal ideal in $\hat{R}_\mathfrak{p}$.

We denote by $H(\Lambda)$ the two-sided class number of $\Lambda$, that is, the order of the group consisting of the locally-free two-sided $\Lambda$-ideals modulo the principal two-sided $\Lambda$-ideals. $\mathrm{Aut}(\Lambda)$ will denote the group of automorphisms of $\Lambda$ , that is, the group of (inner) automorphisms of $A$, which map this order onto itself.

Let $\Lambda$ be an $R$-order in the quaternion algebra $A$ over $K$ and $S$ an $R$-order in a separable quadratic $K$-algebra $B$. An $R$-embedding $\varphi : S \to \Lambda$ is called optimal if $\Lambda/\varphi(S)$ is $R$-projective. We write $e(S, \Lambda)$ to denote the embedding number of $S$ into $\Lambda$, that is, the number of optimal embeddings $S \to \Lambda$ if this number is finite. $\Lambda^*$ acts on the set of embeddings $\varphi : S \to \Lambda$ by inner automorphisms, that is, for $\alpha \in \Lambda^*$, $(\alpha \circ \varphi)(s) = \alpha\varphi(s)\alpha^{-1}$, $s \in S$. We denote by $e_*(S, \Lambda)$ the number of $\Lambda^*$-orbits on the set of embeddings of $S$ in $\Lambda$.

Two quadratic forms $f$ and $g$ are equivalent over $R$ if there exists a matrix $M$ in $GL_3(R)$, such that, $M_f = M^t M_g M$. The quadratic forms $f$ and $g$ are in the same genus if they are equivalent over $\hat{R}_\mathfrak{p}$ for each prime ideal $\mathfrak{p} \neq 0$ in $R$.

Let $(L, q)$ and $(L', q')$ be two quadratic $R$-lattices. They are similar, which we denote by $(L, q) \sim (L', q')$, if and only if there is an $R$-linear bijection $\varphi : L \to L'$ and an element $c \in R^*$ such that $q'(\varphi(x)) = cq(x)$ for all $x \in L$.

## 2. Representations by ternary quadratic forms

In this section, we gather some results on representations of totally positive integers by ternary quadratic forms with coefficients in the rings of all integers in totally real algebraic number fields. We follow the presentation in [2], where the corresponding results were obtained for the rational integers. In fact, we only have to change a few details related to the unit groups. For convenience of the reader, we gather the necessary results formulated for arbitrary rings $R$ under consideration and, occasionally, we give the proofs when they have to be modified to this new situation.

Let $\mathrm{Aut}^+(f)$ denote the group of integral automorphisms of $f$ with determinant 1 and $r_f(N)$ the number of integral representations of $N \gg 0$ by $f$, where $N \in R$. It can be checked, without difficulty, that $|\mathrm{Aut}^+(f)|$ is finite.

The following proposition describes a relation between representations of integers by ternary quadratic forms and solutions to quadratic equations in quaternion orders.

**Proposition 2.1.** *Let $f$ be a totally positive definite ternary quadratic form over $R$. There is an $R$-order $\Lambda$ in a quaternion algebra $A$ over $K$ and a totally positive constant $c_f \in R$, such that the integral representations of $N \in R$, $N \gg 0$, by $f$ are in one-to-one correspondence with the solutions $\lambda \in \Lambda$ to $x^2 = -c_f N$.*

A proof can be given along the same lines as in the proof of Prop. 3.2 in [2] (which treats the case of the rational integers). We will only give a description of $\Lambda$ and $c_f$. Let

$$f(x_1, x_2, x_3) = a_{11}x_1^2 + a_{22}x_2^2 + a_{33}x_3^2 + a_{12}x_1x_2 + a_{13}x_1x_3 + a_{23}x_2x_3,$$

where $a_{ij} \in R$. Let $V = Ke_1 + Ke_2 + Ke_3$, $q(\sum_{i=1}^3 x_i e_i) = f(x_1, x_2, x_3)$ and $T(x,y) = q(x+y) - q(x) - q(y)$. Let $L = Re_1 + Re_2 + Re_3$ and $L^{\#} = \{v \in V : T(v, L) \subseteq R\}$. Then $\Lambda = C_0(L^{\#}, c_0 q)$ and $c_f = \frac{c_0^2}{2\det(M_f)}$, where $c_0 = \frac{2\det(M_f)}{\Omega_f}$.

The relation between $f$ and the corresponding order $\Lambda$ in the proposition leads to the following main result of this section, which can be used for computations of the representation numbers by $f$:

**Theorem 2.2.** *Let $f$ be a totally positive definite ternary quadratic form and $\Lambda$ the quaternion order corresponding to $f$ according to Prop.* 2.1. *Let $f_1 = f, \dots, f_t$ represent the classes in the genus of $f$. Then*

$$\sum_{i=1}^{t} \frac{r_{f_i}(N)}{|\mathrm{Aut}^+(f_i)|} = \delta_\Lambda \sum_S \frac{1}{|S^*/R^*|} h(S) e_{U(\Lambda)}(S, \Lambda),$$

*where $\delta_\Lambda = \frac{|\Lambda^*/R^*|}{|\mathrm{Aut}(\Lambda)| H(\Lambda)}$, the sum is taken over all $R$-orders $S$ such that $R[\sqrt{-c_f N}] \subseteq S \subset K(\sqrt{-c_f N})$ and $S$ is a maximal commutative suborder of $\Lambda$.*

We give a short account of the proof, which needs slight modifications of the arguments given in [2]. First of all, we have the following well-known relation between quadratic lattices and quaternion orders (see [14], Satz 8):

**Proposition 2.3.** *Let $A$ be a quaternion $K$-algebra and $\Lambda$ an $R$-order in $A$ with reduced discriminant $d(\Lambda) = (d_\Lambda)$, $d_\Lambda \in R$. Let*

$$A_0 = \{x \in A : tr(x) = 0\}$$

*and*

$$\Lambda^{\#} = \{x \in A : tr(x\Lambda) \subseteq R\}.$$

*Then $L = \Lambda^{\#} \cap A_0$ is an $R$-lattice on $A_0$. Furthermore,*

$$q(x_1 f_1 + x_2 f_2 + x_3 f_3) = d_\Lambda nr(x_1 f_1 + x_2 f_2 + x_3 f_3),$$

*where $f_1, f_2, f_3$ is an $R$-basis for $L$ and $nr = nr_{A/K}$ denotes the reduced norm, is a ternary quadratic form such that $\Lambda \cong C_0(L, q)$.*

Prop. 2.3 and straightforward calculations give the following result:

**Proposition 2.4.** *There is a one-to-one correspondence described in Prop. 2.3 between similarity classes of quadratic $R$-lattices $(L, q)$, where $q$ is a ternary non-degenerate form, and isomorphism classes of quaternion orders over $R$.*

Let $L = Re_1 + Re_2 + Re_3$ and let $q$ be a quadratic form defined on $L$. Define $f$ by $f(x_1, x_2, x_3) = \sum a_{ij} x_i x_j = q(x_1 e_1 + x_2 e_2 + x_3 e_3)$ and let $\Lambda = C_0(L^{\#}, c_0 q)$. Let $\sigma : L \to L$ be $R$-linear, $\sigma(L) = L$ and $q(\sigma(l)) = cq(l)$ for some $c \in R^*$ and all $l \in L$. Denote by $M$ the matrix representing $\sigma$ in the basis $e_1, e_2, e_3$. We have $M^t M_q M = cM_q$, so $(\det(M))^2 = c^3$, which implies that $c = \tilde{c}^2$ for some $\tilde{c} \in R^*$. We can now define $\sigma_{\tilde{c}} : L \to L$, where $\sigma_{\tilde{c}}(e_i) = \varepsilon \tilde{c}^{-1} \sigma(e_i)$, $\varepsilon$ is 1 if $\det(M) > 0$ and $-1$ otherwise. Let $\tilde{M}$ be the matrix for $\sigma_{\tilde{c}}$. We have $\sigma_{\tilde{c}}(L) = L$, $\det(\tilde{M}) = 1$ and $q(\sigma_{\tilde{c}}(l)) = q(l)$ for all $l \in L$. Using this, we find that $|\mathrm{Aut}(\Lambda)| = |\mathrm{Aut}^+(f)|$. Also note that for $f_i$ in the genus of $f$, the determinants of $M_{f_i}$ and $M_f$ are equal up to multiplication by a unit in $R$. Moreover, $\Omega_{f_i}$ and $\Omega_f$ are defined up to multiplication by a unit, so $c_{f_i}$ can be chosen equal to $c_f$. Now we have:

**Lemma 2.5.** *Let $(L_1, q_1) = (L, q), \ldots, (L_t, q_t)$ represent all classes in the genus of $(L, q)$. Then the orders $\Lambda_1 = \Lambda, \ldots, \Lambda_t$, constructed as in Prop.* 2.1*, represent all the classes in the genus of* $\Lambda$.

*Proof.* Since $(L_1, q_1) = (L, q), \ldots, (L_t, q_t)$ represent all classes in the genus of $(L, q)$, we know that $(L_1^{\#}, c_0 q_1), \ldots, (L_t^{\#}, c_0 q_t)$ will represent all classes in the genus of $(L^{\#}, c_0 q)$. It is clear that the orders $\Lambda_i = C_0(L_i^{\#}, c_0 q_i)$ and $\Lambda_j = C_0(L_j^{\#}, c_0 q_j)$, $i \neq j$ will represent different classes in the same genus. Assume that $\Lambda'$ and $\Lambda = C_0(L^{\#}, c_0 q)$ are in the same genus . Then

$d(\Lambda) = d(\Lambda')$. Using Prop. 2.3, we have $\Lambda' \cong C_0(L', q')$ and $\Lambda \cong C_0(L'', q'')$, where $q' = d_{\Lambda'} nr_{A/K}$ and $q'' = d_\Lambda nr_{A/K}$. Let $M_{q'}$ and $M_{q''}$ be matrices corresponding to the lattices $(L', q')$ and $(L'', q'')$ respectively. We find that we may choose $d_\Lambda$ and $d_{\Lambda'}$ so that the determinants $\det(M_{q'})$ and $\det(M_{q''})$ only differ by the square of a unit in $R^*$. This implies that $(L', q')$ and $(L'', q'')$ are in the same genus, so $\Lambda'$ is isomorphic to one of the orders $\Lambda_i$. $\square$

Finally, we need the following result (see [2], p.204):

**Proposition 2.6.** *Let $\Lambda_1 = \Lambda, \ldots, \Lambda_t$ represent all the isomorphism classes in the genus of $\Lambda$. If $S$ is a maximal commutative suborder of $\Lambda$, then*

$$\sum_{i=1}^{t} H(\Lambda_i) e_*(S, \Lambda_i) = h(S) e_{U(\Lambda)}(S, \Lambda),$$

*where $H(\Lambda_i)$ is the two-sided class number of $\Lambda_i$, $h(S)$ is the locally free class number of $S$ and $e_{U(\Lambda)}(S, \Lambda) = \prod_{\mathfrak{p}} e_*(\hat{S}_{\mathfrak{p}}, \hat{\Lambda}_{\mathfrak{p}})$, $\mathfrak{p} \in Spec(R)$, $\mathfrak{p} \neq (0)$.*

We are now ready to prove Theorem 2.2:

*Proof.* Let $S_0 = R[\sqrt{-c_f N}]$. Then the integral representations of $N$ by $f$, where $N \gg 0$ and $f$ is as in Prop. 2.1, are in one-to-one correspondence with all embeddings $S_0 \to \Lambda$. Notice that each embedding can be extended to an optimal embedding of an $R$-order $S$ such that $S_0 \subseteq S \subset K(\sqrt{-c_f N})$. We have $r_f(N) = \sum_S e(S, \Lambda)$.

The isotropy group for $\varphi$ under the action of $\Lambda^*$ by inner automorphisms consists of all elements $\alpha$ in $\Lambda^*$ such that $\alpha \circ \varphi = \varphi$, that is, those elements $\alpha \in \Lambda$ which commute with each element in $\varphi(S)$ i.e. the isotropy group is $K\varphi(S) \cap \Lambda^*$. Since $\varphi$ is an optimal embedding $K\varphi(S) \cap \Lambda^* \cong S^*$ and the number of elements in each orbit of $\Lambda^*$ is $[\Lambda^* : S^*]$. We know that $[\Lambda^* : S^*] < \infty$ since $[\Lambda^* : R^*] < \infty$, see [7], Satz 2. Thus, we have the equality

$$e(S, \Lambda) = [\Lambda^* : S^*] e_*(S, \Lambda) = [\Lambda^*/R^* : S^*/R^*] e_*(S, \Lambda) \tag{2.7}$$

Using (2.7) and the expression of $r_{f_i}$ by $e(S, \Lambda_i)$, we get

$$\begin{aligned} \sum_{i=1}^{t} \frac{r_{f_i}(N)}{|\mathrm{Aut}^+(f_i)|} &= \sum_{i=1}^{t} \sum_{S} \frac{e(S, \Lambda_i)}{|\mathrm{Aut}(\Lambda_i)|} \\ &= \sum_{i=1}^{t} \sum_{S} \frac{|\Lambda_i^*/R^*|}{|S^*/R^*||\mathrm{Aut}(\Lambda_i)|H(\Lambda_i)} H(\Lambda_i) e_*(S, \Lambda_i). \end{aligned} \tag{2.8}$$

Using similar arguments as in [2], Prop. 3.5, we find that the first factor in this expression $|\Lambda_i^*/R^*|/H(\Lambda_i)|\mathrm{Aut}(\Lambda_i)|$ is the same for all $i$. Interchanging the summation order in (2.8) and applying 2.6, we get the desired result. □

We make the following well-known observation:

**Lemma 2.9.** *Let $f$ be a totally positive definite ternary quadratic form and let $\Lambda$ be the quaternion order constructed as in Prop. 2.1. The primitive solutions correspond to optimal embeddings of $S = R[\sqrt{-c_f N}]$ in $\Lambda$.*

*Proof.* Let $\Lambda = R + RE_1 + RE_2 + RE_3$. We have an embedding $\varphi : S \to \Lambda$, where $\varphi(\sqrt{-c_f N}) = \lambda$, $\lambda^2 = -c_f N$ and $\varphi(S) = R + R\lambda$. Since $R + R\lambda \subset \Lambda$ and $R$ is PID, there exists an $R$-basis, $a_0, a_1, a_2, a_3$, for $\Lambda$ such that $\varphi(S) = Rd_0 a_0 + Rd_1 a_1$, where $d_0, d_1 \in R$ and $d_0 | d_1$. We have

$$\Lambda/\varphi(S) \cong R/(d_0) \oplus R/(d_1) \oplus R^2.$$

Hence, $\Lambda/\varphi(S)$ is $R$-projective if and only if $d_0, d_1 \in R^*$. Let $f(r_1, r_2, r_3) = N$ be a primitive solution, that is, $GCD(r_1, r_2, r_3) = 1$. Using Prop. 2.1, we get $\lambda = r_0 + r_1 E_1 + r_2 E_2 + r_3 E_3$ such that $\lambda^2 = -c_f N$. We know that $1 = r_0' d_0 a_0 + r_1' d_1 a_1$ and $\lambda = r_0'' d_0 a_0 + r_1'' d_1 a_1$. Then $d_0 | 1$, since $d_0 | d_1$, so $d_0 \in R^*$. We also know that

$$\begin{vmatrix} r_0' & r_0'' \\ r_1' & r_1'' \end{vmatrix} = r_0' r_1'' - r_0'' r_1' \in R^*.$$

We observe that $\lambda r_0' - r_0'' = (r_0' r_1'' - r_0'' r_1') d_1 a_1$. Then $d_1 | r_0'$ and $d_1 | r_0''$, since $GCD(r_1, r_2, r_3) = 1$, so $d_1$ divides the determinant and we find that $d_1 \in R^*$. Hence the embedding of $S$ in $\Lambda$ is optimal. Now we assume that $f(r_1, r_2, r_3) = N$ is not primitive. Let $d = GCD(r_1, r_2, r_3)$. Then we know that $d | r_i$, $i = 0, 1, 2, 3$, where $r_i$ denote the coefficients of $\lambda \in \Lambda$. But then $\varphi(S) = R + R\lambda \subset R + R\frac{\lambda}{d}$, that is, $\varphi(S)$ is not a maximal commutative subring of $\Lambda$. Hence $\Lambda/\varphi(S)$ is not projective. □

Denote by $r_f^0(N)$ the number of primitive solutions to $f(x_1, x_2, x_3) = N$. Using Lemma 2.9, we have a Corollary, which gives us a formula for the number of primitive representations of $N$ by $f$ when $t = 1$.

**Corollary 2.10.** *With the same notation as in Prop. 2.2,*

$$\sum_{i=1}^{t} \frac{r_{f_i}^0(N)}{|\mathrm{Aut}^+(f_i)|} = \delta_\Lambda \frac{1}{|S^*/R^*|} h(S) e_{U(\Lambda)}(S, \Lambda),$$

*where $S = R[\sqrt{-c_f N}]$.*

## 3. Stability of the embedding numbers

The main objective of this section is Thm. 3.2 which is analogous to Thm. 3.4. in [4]. Unfortunately, we were not able to eliminate the restriction to quadratic fields $\mathbb{Q}(\sqrt{d})$ with $d \not\equiv 1$ $(mod\ 8)$. The proof depends on a stability property of the embedding numbers of some commutative quadratic orders into quaternion orders over complete discrete valuation rings. We start with the following well-known fact, which we need in the sequel:

**Lemma 3.1.** *Let $K = \mathbb{Q}(\sqrt{d})$, where $d \in \mathbb{Z}$, $d > 0$ and $d$ is square-free. Denote by $R$ the integers in $K$. Let $S = R[\sqrt{-\alpha}]$, where $\alpha \in R$, $\alpha \notin R^*$ and $\alpha \gg 0$. Then $S^* = R^*$.*

*Proof.* Let $K' = K(\sqrt{-\alpha})$ and let $^-\colon K' \to K'$ denote complex conjugation. Let $\epsilon \in S^*$. Then the map $\epsilon \to \frac{\epsilon}{\bar{\epsilon}}$ will send the units in $S^*$ to roots of unity in $S^*$ since $K'$ is a CM-field. So $\epsilon = \varepsilon_n \bar{\epsilon}$, where $\varepsilon_n$ denote an $n$:th root of unity. Then the minimum polynomial $m_{\varepsilon_n}$ is of degree $\varphi(n)$, where $\varphi$ is the Euler function. In our case, $\varphi(n)|4$, so the only possibilities are $n = 2, 3, 4, 5, 6, 8, 10, 12$. It is then easy to check that $\{-1, 1\}$ are the only roots of unity in $S$. But $\varepsilon_n = -1$ is impossible since $\alpha \notin R^*$. Hence we have $\epsilon = \bar{\epsilon}$ so $\epsilon \in R^*$. □

**Theorem 3.2.** *Let $K = \mathbb{Q}(\sqrt{d})$, where $d$ is a positive square-free rational integer. Denote by $R$ the ring of integers in $K$. Let $d \not\equiv 1$ $(mod\ 8)$ be such that $R$ is a principal ideal domain. Let $f$ be a totally positive definite ternary quadratic form over $R$ and let $\Lambda = \Lambda_f$ be the corresponding order according to Prop. 2.1. Assume that $G(\Lambda)$ is a Bass order (see Section 1) and let*

$$\sum_{i=1}^{t} \frac{r^0_{f_i}(N)}{|\mathrm{Aut}^+(f_i)|} = \gamma(N)h(S),$$

*as in Cor. 2.10, $S = R[\sqrt{-c_f N}]$ and*

$$\gamma(N) = \frac{|\Lambda^*/R^*|}{|\mathrm{Aut}(\Lambda)|H(\Lambda)|S^*/R^*|} \prod_{\mathfrak{p}} e_*(\hat{S}_{\mathfrak{p}}, \hat{\Lambda}_{\mathfrak{p}}).$$

*Then there is a positive rational integer $M_0$ such that $\gamma$ has the following property: Let $c_f N = N_0^2 N_1$ and $c_f N' = N_0'^2 N_1'$ be two totally positive non-units in $R$, where $N_0, N_1, N_0', N_1' \in R$ and $N_1, N_1'$ are square-free, such that for all $\mathfrak{p}|d(\Lambda)$ we have*

$$v_{\mathfrak{p}}(N_0) = v_{\mathfrak{p}}(N_0') \ or\ min(v_{\mathfrak{p}}(N_0), v_{\mathfrak{p}}(N_0')) \geq v_{\mathfrak{p}}(M_0) \tag{3.3}$$

$$N_1 \mathfrak{p}^{-v_{\mathfrak{p}}(N_1)} \equiv N_1' \mathfrak{p}^{-v_{\mathfrak{p}}(N_1')} \pmod{\mathfrak{p}^{2v_{\mathfrak{p}}(2)+1}} \tag{3.4}$$

$$N_1 \equiv N_1' \pmod{16} \tag{3.5}$$

*where $v_{\mathfrak{p}}$ denotes the $\mathfrak{p}$-adic valuation. Then $\gamma(N) = \gamma(N')$ and furthermore, one may choose $M_0$ to be the positive generator of the ideal $(d(\Lambda)) \cap \mathbb{Z}$.*

*Proof.* Let $L = K(\sqrt{-c_f N}) = K(\sqrt{-N_1})$ and $L' = K(\sqrt{-N_1'})$. If $c_f N \notin R^*$, then $|S^*/R^*| = 1$ (according to Lemma 3.1) and the factor

$$\frac{|\Lambda^*/R^*|}{|\mathrm{Aut}(\Lambda)| H(\Lambda) |S^*/R^*|}$$

is independent of $N$.

Denote by $\Delta(L/K)$ the discriminant of the extension $K \subseteq L$. According to Prop. 2.4 and 2.5 in [4], we have $e_*(\hat{S}_{\mathfrak{p}}, \hat{\Lambda}_{\mathfrak{p}}) = e_*(\hat{S}'_{\mathfrak{p}}, \hat{\Lambda}_{\mathfrak{p}})$ if

$$\Delta(\hat{L}_{\mathfrak{p}}/\hat{K}_{\mathfrak{p}}) \equiv \Delta(\hat{L}'_{\mathfrak{p}}/\hat{K}_{\mathfrak{p}}) \pmod{\mathfrak{p}^{\delta(\hat{L}_{\mathfrak{p}}, \hat{L}'_{\mathfrak{p}})}} \tag{3.6}$$

and the conductors $\mathfrak{f}_{\mathfrak{p}}$ and $\mathfrak{f}'_{\mathfrak{p}}$ of $\hat{S}_{\mathfrak{p}}$ and $\hat{S}'_{\mathfrak{p}}$ with respect to the maximal orders in $\hat{L}_{\mathfrak{p}}$ and $\hat{L}'_{\mathfrak{p}}$ satisfy

$$\mathfrak{f}_{\mathfrak{p}} \equiv \mathfrak{f}'_{\mathfrak{p}} \pmod{\mathfrak{p}^{i(\mathfrak{p})}}, \tag{3.7}$$

where $\delta(\hat{L}_{\mathfrak{p}}, \hat{L}'_{\mathfrak{p}}) = 2v_{\mathfrak{p}}(2) + 1 + \min(v_{\mathfrak{p}}(\Delta(\hat{L}_{\mathfrak{p}}/\hat{K}_{\mathfrak{p}})), v_{\mathfrak{p}}(\Delta(\hat{L}'_{\mathfrak{p}}/\hat{K}_{\mathfrak{p}})))$ and $i(\mathfrak{p})$ is a given rational non-negative integer such that $i(\mathfrak{p}) \leq v_{\mathfrak{p}}(d(\Lambda))$. Hence the factor

$$\prod_{\mathfrak{p}} e_*(\hat{S}_{\mathfrak{p}}, \hat{\Lambda}_{\mathfrak{p}})$$

depends on the conductor $\mathfrak{f}$ of $S$ with respect to the maximal order in $L$ and the relative discriminant $\Delta(L/K)$. Let $R'$ denote the integers in $L$. $R$ is a PID, so $R' = R + R\omega$, for some $\omega \in R'$. For a suborder $O \subseteq R'$, we have $O = R + Ra\omega$ for some $a \in R$. Then $\mathfrak{f} = (a)$. Using the relation $D(O) = \mathfrak{f}^2 \Delta(L/K)$, where $D(O)$ denotes the discriminant of the order $O$, and the fact that $\{1, \sqrt{-N_1}\}$ is a basis for $L$ over $K$, we find that $\Delta(L/K) = (c^2 N_1)$ and $\mathfrak{f} = (\frac{2}{c} N_0)$ for some $c \in R$ such that $c|2$. We use Thm. 1 in [20] and the classification of possible cases given in [8] in Tables A-C to see, that the factor $c$ of the relative discriminant will be the same for $N_1$ and $N_1'$ if $N_1 \equiv N_1' \pmod{16}$.

Assume that the prime $\mathfrak{p}$ does not divide $d(\Lambda)$ and let $\Lambda_m$ denote a maximal order in $A$ such that $\Lambda \subseteq \Lambda_m$. Then $\mathfrak{p}$ does not divide $d(\Lambda_m)$, so $\hat{A}_{\mathfrak{p}} = A \otimes \hat{K}_{\mathfrak{p}}$ is split (see e.g. Cor. 5.3 in [21]). Since $\mathfrak{p}$ does not divide $d(\Lambda)$, we also know that $\hat{\Lambda}_{\mathfrak{p}}$ is a maximal order and thereby hereditary ($d(\hat{\Lambda}_{\mathfrak{p}})$ is square-free). According to Prop. 3.1.(b) in [3], we have $e_*(\hat{S}_{\mathfrak{p}}, \hat{\Lambda}_{\mathfrak{p}}) = 1$.

Let $\mathfrak{p}|d(\Lambda)$. Then (3.3), (3.4) and (3.5) will ensure that the conditions (3.6) and (3.7) are satisfied. Hence $\gamma(N) = \gamma(N')$. The choice of $M_0$ as the positive generator of $d(\Lambda) \cap \mathbb{Z}$ is possible since $i(\mathfrak{p}) \leq v_{\mathfrak{p}}(d(\Lambda))$.

□

**Corollary 3.8.** *With the notation as in Thm.* 3.2*, there exist positive rational integers $M_0$ and $M_1$ such that the value of $\gamma(N) = \gamma(N_0, N_1)$ is determined by the residues of $N_0$ modulo $M_0$ and $N_1$ modulo $M_1$.*

*Proof.* Let $d_1$ denote the product of all different primes $\mathfrak{p}$ in $R$ such that $\mathfrak{p}$ divides $d_\Lambda$ but $\mathfrak{p}$ does not divide 2. It follows from Thm. 3.2 that it is possible to choose $M_0$ and $M_1$ as the positive generators of the ideals $d(\Lambda) \cap \mathbb{Z}$ and $(4d_1)^2 \cap \mathbb{Z}$ respectively. □

## 4. The sum of three squares

Let $K = \mathbb{Q}(\sqrt{5})$, $R = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ and let $f : R^3 \to R$, $f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$. Denote by $\Lambda_f$ the quaternion order $C_0(L^\#, c_0 q)$ corresponding to $f$ according to Thm. 2.1 and denote by $A$ the quaternion algebra $K \otimes_R \Lambda_f$. We have $c_f = 1$ and $\Lambda_f = R + RE_1 + RE_2 + RE_3$, where $E_i^2 = E_j^2 = -1$ and $E_iE_j = -E_jE_i = -E_k$, where $i, j, k$ is an even permutation of $1, 2, 3$. The type number of $C_0(f) \cong \Lambda_f$ is 1, since the type number of $f$ is 1 (see Satz 24 in [6] or, for an algebraic argument, [11], p. 685). It is not difficult to check that $\Lambda_f$ is a Bass order using the condition given in [4], p. 315.

It was proved in [12] that every totally positive number $N$ in $R = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ can be represented as a sum of three squares. We will now give a proof of this, based on algebraic methods. Moreover, we will prove that there is a primitive representation for every totally positive element in $R$.

**Theorem 4.1.** *Every totally positive number $N$ in $R = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ can be represented by $f : R^3 \to R$, where*

$$f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2.$$

*Moreover, there is always $(x_1, x_2, x_3) \in R^3$ such that $GCD(x_1, x_2, x_3) = 1$ and $f(x_1, x_2, x_3) = N$.*

*Proof.* Let $\Lambda$ denote the order corresponding to $f$, described above. Let $N \in R$ be totally positive with $N = N_1 N_0^2$, where $N_0, N_1 \in R$ and $N_1$ is square-free. Let $L = K(\sqrt{-N_1})$ and let $\omega = \frac{1+\sqrt{5}}{2}$. It can then be checked that the discriminant $\Delta(L/K) = -N_1$ if $-N_1 \equiv 1,\ \ \omega + 1$ or $(\omega + 1)^2$ and $\Delta(L/K) = -4N_1$ otherwise. $A$ is a totally definite quaternion algebra so it ramifies at both infinite primes. We know that $A$ ramifies at an even number of primes and that the finite primes where $A$ ramifies divide the reduced discriminant of the maximal orders (see [21], Chap. II, Cor. 5.3 and Chap. III, Thm. 3.1). Hence, $A$ ramifies only at the infinite primes since $d_\Lambda = 4$. Furthermore, $\hat{\Lambda}_\mathfrak{p}$ is maximal for all primes $\mathfrak{p} \neq 2$ in $R$ but not for $\mathfrak{p} = 2$.

Using Lemma 2.9 and Cor. 2.10, all we need to show is that for a totally positive integer $N \in R$ it is possible to embed $S = R[\sqrt{-N}]$ as a maximal commutative suborder of $\Lambda$, that is, $e_{U(\Lambda)}(S, \Lambda) \neq 0$. We start by observing that by Thm. 3.2. in [21], we have $e_*(\hat{S}_\mathfrak{p}, \hat{\Lambda}_\mathfrak{p}) = 1$, for all $\mathfrak{p} \neq 2$ and all orders $S$ in a commutative algebra of degree two over $K$, since $\hat{\Lambda}_\mathfrak{p}$ is maximal.

Using Lemma 6 in [10] we find that $e_{(2)}(\Lambda_f) = 0$ since the discriminant $\delta(\lambda) = (tr(\lambda))^2 - 4nr(\lambda) = -4(r_1^2 + r_2^2 + r_3^2) \in 2\hat{R}_2$ for all elements $\lambda = r_0 + r_1E_1 + r_2E_2 + r_3E_3$ in $\hat{\Lambda}_{f(2)}$. If 2 divides $\Delta(L/K)$, then $e_*(\hat{S}_2, \hat{\Lambda}_2) \neq 0$, by 3.14 in [3] if $\hat{S}_2$ is maximal in $\hat{L}_2$, since $L$ is ramified over $K$, and by 3.17 in [3] if it is not maximal. If 2 does not divide $\Delta(L/K)$, then the maximal order of $L$ will be $R[\frac{a+\sqrt{-N_1}}{2}]$, where $a = 1$ for $-N_1 \equiv 1$, $a = \omega + 1$ for $-N_1 \equiv (\omega+1)^2$ and $a = (\omega+1)^2$ for $-N_1 \equiv \omega + 1$. We have $S = R[\sqrt{-N}]$. Hence, $\hat{S}_2$ will not be maximal in $\hat{L}_2$, so by 3.17 in [3], we have $e_*(\hat{S}_2, \hat{\Lambda}_2) \neq 0$. Hence $e_{U(\Lambda)}(S, \Lambda) \neq 0$. □

Finally we shall find a formula for the number of primitive representations of $N$ by $f$. We start by observing that if $N \in R^*$ and $N \gg 0$, then $N$ is a square. It is then easy to check that $r_f^0(N) = 6$.

**Theorem 4.2.** *Let $N$ be a totally positive non-unit in $R = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ and let $f(x_1, x_2, x_3) = x_1^2 + x_2^2 + x_3^2$. Let $N = N_0^2 N_1$, where $N_0, N_1 \in R$ and $N_1$ is square-free. Then the number of primitive representations of $N$ by $f$, $r_f^0(N)$, is given by*

$$r_f^0(N) = \begin{cases} 32h(S) & \text{if } N_0 \not\equiv 0 \pmod 2 \text{ and } N_1 \equiv 3, 7, 3+3\omega, 6+\omega, \\ & \qquad 6+5\omega, 7+7\omega \pmod 8, \\ 24h(S) & \text{if } N_0 \equiv 0 \pmod 2 \\ & \text{or } N_0 \not\equiv 0 \pmod 2 \text{ and } N_1 \equiv 2+\omega, 2+5\omega, 3+4\omega, \\ & \qquad 3+7\omega, 7+3\omega, 7+4\omega \pmod 8, \\ 12h(S) & \text{otherwise,} \end{cases}$$

*where $\omega = \frac{1+\sqrt{5}}{2}$.*

*Proof.* Assume that $N \notin R^*$. We have $|\mathrm{Aut}^+(f)| = 24$. Using Cor. 3.8, we may choose $M_0 = 4$ and $M_1 = 16$. We also observe that for $N_1$ not divisible by 2, $M_1 = 8$ suffices (see Tables A-C in [8], Thm. 1 in [20] and Thm. 3.2). We choose a suitable limited set of numbers $N$ to represent all congruence classes modulo $M_0$ and $M_1$. We observe that $0 < a$, $0 < m < a$ and $\frac{-a}{\sqrt{5}} < n < \frac{a}{\sqrt{5}}$ for $N = \frac{a+b\sqrt{5}}{2} = x_1^2 + x_2^2 + x_3^2$ and $0 \neq x_i^2 = \frac{m+n\sqrt{5}}{2}$ ($m \equiv n$

and $a \equiv b \pmod 2$)). Using this we compute the number of primitive representations of $N$ by $f$, by exhaustive search, for this finite set. We then calculate the class numbers $h(R[\sqrt{-N}])$. Let $S = R[\sqrt{-N}]$ and let $S_0$ denote the maximal order in $K(\sqrt{-N})$. We use the following relation

$$h(S) = \frac{h(S_0)}{[S_0^* : S^*]} \prod_{\mathfrak{p}|\mathfrak{f}} [\hat{S_0}_{\mathfrak{p}}^* : \hat{S}_{\mathfrak{p}}^*], \tag{4.3}$$

where $\mathfrak{f}$ is the conductor for $S$ with respect to $S_0$ and $\mathfrak{p}$ denotes prime ideals in $R$ (see [13], Thm. 12.12 and [19], 3.4). Functions in GP-PARI are used to calculate the class numbers and the number of roots of unity in $S_0$ as well as the behaviour of prime ideals $\mathfrak{p} \subset R$, such that $\mathfrak{p} \mid \mathfrak{f}$, in $K[\sqrt{-N}]$. We find that the only possible values for $\gamma(N)$ are $\frac{1}{2}, 1$ and $\frac{4}{3}$. $\square$

## 5. Quadratic forms corresponding to maximal orders

In this section, we use a somewhat different method in order to study the number of integral representations by ternary quadratic forms. We start with maximal $R$-orders $\Lambda$ in totally definite quaternion algebras over quadratic real number fields $\mathbb{Q}(\sqrt{m})$ such that $d(\Lambda) = R$ and $h_\Lambda = 1$. There are only four such cases and these are $m = 2, 5, 13, 17$, see [21] p. 155. We will denote the maximal orders by $\Lambda^{(m)}$. We have $\Lambda^{(m)} \cong C_0(f_m)$ with $m$ and $f_m$ as in the following table.

(5.1)

| $m$ | $f_m$ |
|---|---|
| 2 | $x_1^2 + x_2^2 + x_3^2 + \sqrt{2}x_1x_2 + x_1x_3$ |
| 5 | $x_1^2 + x_2^2 + x_3^2 + \omega x_1x_2 + \omega^{-1}x_1x_3$ |
| 13 | $2x_1^2 + 2x_2^2 + x_3^2 + \sqrt{13}x_1x_2 + x_1x_3$ |
| 17 | $6x_1^2 + 3x_2^2 + x_3^2 + 2\sqrt{17}x_1x_2 + x_1x_3$ |

We would now like to find the number of primitive representations of a totally positive number $N$ by $f_m$. We start with the following observation.

**Lemma 5.2.** *Let $\Lambda = C_0(f)$ be an $R$-order, in $A$, such that $d(\Lambda) = R$. Let $L = \Lambda \cap A_0$ and $L^\# = \Lambda^\# \cap A_0$, with notation as in Prop. 2.3. Then $(L, nr_{A/K}) \cong (L^\#, nr_{A/K})$.*

*Proof.* Let $f(r_1, r_2, r_3) = \sum a_{ij} r_i r_j$ and let $1, E_1, E_2, E_3$ denote an $R$-basis for $\Lambda$. We have $\Lambda \cong C_0(L^{\#}, nr_{A/K})$ by Prop. 2.3. $\Lambda^{\#} = \{x \in A : tr(x\Lambda) \subseteq R\}$, so $\Lambda \subseteq \Lambda^{\#}$ and $L \subseteq L^{\#}$. We also know that $L^{\#} = RF_1 + RF_2 + RF_3$, where $F_i = a_{ii}a_{jk} + a_{ij}a_{ik} - 2a_{ii}E_i - a_{ij}E_j - a_{ik}E_k$, so $F_i \in \Lambda$ for $i = 1, 2, 3$. Hence $L^{\#} \subseteq L$ and $(L, nr_{A/K}) \cong (L^{\#}, nr_{A/K})$. □

**Proposition 5.3.** *For $m = 2, 5, 13, 17$ and $f_m$ as in table* (5.1), *the number of representations of totally positive number $N$ by $f_m$ is given by*

$$r_{f_m}(N) = |\Lambda^{(m)*}/R^*| \sum_S \frac{h(S)}{|S^*/R^*|},$$

*where we sum over $R$-orders $S$ such that $R[\sqrt{-N}] \subseteq S \subset K(\sqrt{-N})$ and $S$ is a maximal commutative suborder of $\Lambda^{(m)}$.*

*Proof.* For an element $\lambda \in \Lambda^{(m)}$, we have $\lambda^2 - tr(\lambda)\lambda + nr(\lambda) = 0$, so $\lambda^2 = -nr(\lambda)$ when $\lambda \in L = \Lambda \cap A_0$. Using the condition $tr(\lambda) = 0$ to substitute one of the variables in the expression for $nr(x_0 + x_1E_1 + x_2E_2 + x_3E_3)$ we get a ternary quadratic form $f : R^3 \to R$. We then have a one-to-one correspondence between representations of $N$ by $f$ and the embeddings of $S_0 = R[\sqrt{-N}]$ in $\Lambda^{(m)}$. We observe that each embedding can be extended to an optimal embedding of an $R$-order $S$, where $S_0 \subseteq S \subset K(\sqrt{-N})$, so $r_f(N) = \sum_S e(S, \Lambda^{(m)})$. Using (2.7), Prop. 2.6 and the fact that $h_{\Lambda^{(m)}} = 1$, we find that

$$r_f(N) = |\Lambda^{(m)*}/R^*| \sum_S \frac{h(S)}{|S^*/R^*|} e_{U(\Lambda^{(m)})}(S, \Lambda^{(m)}).$$

Since $\Lambda^{(m)}$ is a maximal order and $\hat{A}_{\mathfrak{p}}$ is split for all finite primes $\mathfrak{p}$, we have $e_{U(\Lambda^{(m)})}(S, \Lambda^{(m)}) = 1$ (see [3], Prop. 3.1 b)). Hence

$$r_f(N) = |\Lambda^{(m)*}/R^*| \sum_S \frac{h(S)}{|S^*/R^*|}.$$

Using the lemma above and observing that $C_0(f_m) \cong C_0(L^{\#}, nr_{A/K})$ (by Prop. 2.3) we have $r_f(N) = r_{f_m}(N)$ and $r_f^0(N) = r_{f_m}^0(N)$. □

We are interested in the number of primitive representations of a totally positive integer $N$ by $f$. We have to determine the maximal commutative suborders $S$ of $\Lambda^{(m)}$ corresponding to primitive representations by $f$ and also calculate $\frac{|\Lambda^{(m)*}/R^*|}{|S^*/R^*|}$ to get an explicit formula.

We will describe the calculations for the case $m = 13$. Calculating the norm of an element $\lambda = r_0 + r_1E_1 + r_2E_2 + r_3E_3$ in $C_0(f_{13})$ and using the condition $tr(\lambda) = 0$, we get the quadratic form

$$f(x_1, x_2, x_3) = 2x_1^2 + 7x_2^2 + 17x_3^2 + 2\sqrt{13}x_1x_2 + 11x_1x_3 + 6\sqrt{13}x_2x_3.$$

When we use the condition $tr(\lambda) = 0$, we may choose to substitute a different variable (this would give us an equivalent form). Let $\mu = \frac{1+\sqrt{13}}{2}$. We observe that if $f(r_1, r_2, r_3) = N$, then $\lambda = r_2 + r_1E_1 - (2r_2 + \sqrt{13}r_3)E_2 + r_3E_3$ is such that $\lambda^2 = -N$. Using this correspondence and assuming that we have a primitive representation by $f$ of $N = N_0^2N_1$, where $N_0, N_1 \in R$ and $N_1$ is square-free, we find that $S = R[N_0\frac{a+\sqrt{-N_1}}{2}]$ if $2 \mid GCD(r_1, r_3)$, where $a = 1, 1+\mu, \mu$ for $N_1 \equiv 3, \mu, 1+3\mu \pmod 4$ respectively, and $S = R[\sqrt{-N}]$ otherwise. We also find that an optimal embedding of $S = R[\sqrt{-N}]$ corresponds to a primitive representation of $N$ by $f$ and an optimal embedding of $S = R[N_0\frac{a+\sqrt{-N_1}}{2}]$ gives us a primitive representation of $N$ by $f$ if and only if $2 \nmid N_0$. Hence, for the cases where $2 \nmid N_0$ and $N_1 \equiv 3, \mu, 1+3\mu \pmod 4$, we sum over $S_1 = R[N_0\frac{a+\sqrt{-N_1}}{2}]$ and $S_0 = R[\sqrt{-N}]$. In all other cases only $S_0 = R[\sqrt{-N}]$ will contribute.

To calculate $|\Lambda^{(m)*}/R^*|$, we start by observing that $nr(\lambda) \gg 0$ for $\lambda \in \Lambda^{(m)}$. Hence, for $\lambda \in \Lambda^{(m)*}$, we have $nr(\lambda) = \varepsilon^2 \in R^*$. It is then enough to find the elements $\lambda \in \Lambda^{(m)}$ such that $nr(\lambda) = 1$ and consider them modulo $R^*$. We get $|\Lambda^{(13)*}/R^*| = 12$.

Calculations similar to those in the proof of Lemma 3.1 will give us the value of $|S_i^*/R^*|$ for $i = 0, 1$.

Using the formula

$$r_f^0(N) = |\Lambda^{(m)*}/R^*| \sum_i \frac{h(S_i)}{|S_i^*/R^*|}$$

and the following table, we have the result for $m = 13$.

| $\mathbf{N_1}$ **(mod 4)** | | **Sum over** | $a$ |
|---|---|---|---|
| $3, \mu, 1+3\mu$ | $2 \nmid N_0$ | $S_0 = R[\sqrt{-N}]$<br>$S_1 = R[N_0\frac{a+\sqrt{-N_1}}{2}]$ | 1 for $N_1 \equiv 3$<br>$1+\mu$ for $N_1 \equiv \mu$<br>$\mu$ for $N_1 \equiv 1+3\mu$ |
| otherwise | | $S_0 = R[\sqrt{-N}]$ | |

The values of $|S_i^*/R^*|$ will be

$$|S_1^*/R^*| = \begin{cases} 3 & \text{if } N_1 = 3 \quad \text{and } N_0 \in R^*, \\ 1 & \text{otherwise,} \end{cases}$$

$$|S_0^*/R^*| = \begin{cases} 2 & \text{if } N_1 = 1 \quad \text{and } N_0 \in R^*, \\ 1 & \text{otherwise.} \end{cases}$$

We have to sum over more than one order only when $N_1 \equiv 3, \mu$ or $1+3\mu$ and $2 \nmid N_0$. We will study these cases more closely in order to find a more convenient formula for $r_f^0(N)$. Let $L$ denote $K(\sqrt{-N_1})$ and let $S$ be the maximal order in $L$. Let $\mathfrak{f}_0, \mathfrak{f}_1$ denote the conductors for $S_0, S_1$ with respect to $S$. Using (4.3) we find that $h(S_1) = h(S_0)[S_1^* : S_0^*]c$, where $c = \frac{1}{5}, \frac{1}{3}$ if (2) is prime in $L$ and (2) is split in $L$ respectively ($2 \nmid \mathfrak{f}_1$ since $2 \nmid N_0$). We find that (2) is split for $N_1 \equiv 3, 7, 5+7\mu, 1+3\mu, 4+5\mu, 4+\mu \pmod 8$ and prime for $N_1 \equiv 3+4\mu, 7+4\mu, 5+3\mu, 1+7\mu, \mu, 5\mu \pmod 8$.

The other cases have been calculated using the same techniques (see [1]).

**Proposition 5.4.** *Let $K$ be a real quadratic number field and $R$ its ring of integers. Let $\Lambda = C_0(f)$ be an $R$-order with $d(\Lambda) = R$ and $h_\Lambda = 1$, in a totally definite quaternion algebra over $K$. Then $f$ can be chosen as one of the forms in (5.1) and the number of primitive representations of a totally positive number $N \in R$ by $f$ is given by the following formulas:*

$$r_{f_{13}}^0(N) = \begin{cases} 6h(S_0) & \textit{if } N_1 = 1 \qquad \textit{and } N_0 \in R^* \\ 12h(S_0) & \textit{if } N_1 \not\equiv 3, \mu, 1+3\mu \quad (4) \qquad \textit{and } N \notin R^* \\ & \textit{or } N_1 \equiv 3, \mu, 1+3\mu \quad (4) \qquad \textit{and } 2 | N_0 \\ 16h(S_0) & \textit{if } N_1 \equiv 3, 7, 5+7\mu, 1+3\mu, 4+5\mu, 4+\mu \quad (8) \\ & \qquad \textit{and } 2 \nmid N_0 \\ \frac{72}{5}h(S_0) & \textit{otherwise,} \end{cases}$$

$$r_{f_2}^0(N) = \begin{cases} 18h(S_0) & \textit{if } N_1 = 1 \qquad \textit{and } N_0 \in R^* \\ 24h(S_0) & \textit{if } N_1 \not\equiv 1 \quad (2) \\ & \textit{or } N_1 \equiv 1 \quad (2) \qquad \textit{and } \sqrt{2} \mid N_0 \\ 36h(S_0) & \textit{if } N_1 \equiv 1, 3+2\sqrt{2} \quad (4) \qquad \textit{and } \sqrt{2} \nmid N_0 \\ 40h(S_0) & \textit{if } N_1 \equiv 3, 1+2\sqrt{2} \quad (4\sqrt{2}) \quad \textit{and } \sqrt{2} \nmid N_0 \\ 48h(S_0) & \textit{otherwise,} \end{cases}$$

$$r^0_{f_5}(N)=\begin{cases} 30h(S_0) & \textit{if } N_1=1 \qquad\qquad\qquad\qquad \textit{and } N_0\in R^* \\ 60h(S_0) & \textit{if } N_1\not\equiv 3,2+\omega,3+3\omega \quad (4) \qquad \textit{and } N\notin R^* \\ & \textit{or } N_1\equiv 3,2+\omega,3+3\omega \quad (4) \qquad \textit{and } 2\mid N_0 \\ 72h(S_0) & \textit{if } N_1\equiv 2+\omega,2+5\omega,3+7\omega,7+3\omega,3+4\omega, \\ & \qquad\qquad\qquad 7+4\omega \quad (8) \;\; \textit{and } 2\nmid N_0 \\ 80h(S_0) & \textit{otherwise}, \end{cases}$$

$$r^0_{f_{17}}(N)=\begin{cases} 3h(S_0) & \textit{if } N_1=1 \qquad\qquad\qquad\qquad \textit{and } N_0\in R^* \\ 8h(S_0) & \textit{if } N_1\equiv 1+2\gamma,5+6\gamma,6+\gamma,2+5\gamma \quad (8) \\ & \qquad\qquad\qquad\qquad \textit{and } \mathfrak{p}_1\nmid N_0 \\ & \textit{or } N_1\equiv 3+2\gamma,3+6\gamma,7+3\gamma,7+7\gamma \quad (8) \\ & \qquad\qquad\qquad\qquad \textit{and } \mathfrak{p}_2\nmid N_0 \\ & \textit{or } N_1\equiv 3 \quad (8) \qquad\qquad \textit{and } \mathfrak{p}_i\mid N_0,\ 2\nmid N_0 \\ & \textit{or } N_1\equiv 3+4\gamma \quad (8) \qquad \textit{and } \mathfrak{p}_1\mid N_0,\ \mathfrak{p}_2\nmid N_0 \\ & \textit{or } N_1\equiv 7+4\gamma \quad (8) \qquad \textit{and } \mathfrak{p}_1\nmid N_0,\ \mathfrak{p}_2\mid N_0 \\ \frac{32}{3}h(S_0) & \textit{if } N_1\equiv 3 \quad (8) \qquad\qquad \textit{and } \mathfrak{p}_i\nmid N_0,\ i=1,2 \\ 12h(S_0) & \textit{if } N_1\equiv 5+2\gamma,1+6\gamma,2+\gamma,6+5\gamma \quad (8) \\ & \qquad\qquad\qquad\qquad \textit{and } \mathfrak{p}_1\nmid N_0 \\ & \textit{or } N_1\equiv 7+2\gamma,7+6\gamma,3+3\gamma,3+7\gamma \quad (8) \\ & \qquad\qquad\qquad\qquad \textit{and } \mathfrak{p}_2\nmid N_0 \\ & \textit{or } N_1\equiv 7 \quad (8), \qquad\qquad \textit{and } \mathfrak{p}_i\mid N_0,\ 2\nmid N_0 \\ & \textit{or } N_1\equiv 7+4\gamma \quad (8) \qquad \textit{and } \mathfrak{p}_1\mid N_0,\ \mathfrak{p}_2\nmid N_0 \\ & \textit{or } N_1\equiv 3+4\gamma \quad (8) \qquad \textit{and } \mathfrak{p}_1\nmid N_0,\ \mathfrak{p}_2\mid N_0 \\ 16h(S_0) & \textit{if } N_1\equiv 3+4\gamma,7+4\gamma \quad (8) \;\; \textit{and } \mathfrak{p}_i\nmid N_0,\ i=1,2 \\ 24h(S_0) & \textit{if } N_1\equiv 7 \quad (8) \qquad\qquad \textit{and } \mathfrak{p}_1\nmid N_0,\ \mathfrak{p}_2\nmid N_0 \\ 6h(S_0) & \textit{otherwise}. \end{cases}$$

*where* $\mu=\frac{1+\sqrt{13}}{2}$, $\omega=\frac{1+\sqrt{5}}{2}$, $\gamma=\frac{1+\sqrt{17}}{2}$, $\mathfrak{p}_1=1+\gamma$ *and* $\mathfrak{p}_2=-2+\gamma$.

## References


[1] E. Björkholdt, *Reserch report NO 1997-44*, Göteborg, 1997.

[2] J. Brzezinski, *A combinatorial class number formula.* J. Reine Angew. Math. **402** (1989), 199–210.

[3] J. Brzezinski, *On automorphisms of quaternion orders.* J. Reine Angew. Math. **403** (1990), 166–186.

[4] J. Brzezinski, *On embedding numbers into quaternion orders.* Comment. Math. Helvetici **66** (1991), 302–318.

[5] E. N. Donkar, *On Sums of Three Integral Squares in Algebraic Number Fields.* Am. J. Math. **99** (1977), 1297–1328.

[6] J. Dzewas, *Quadratsummen in reell-quadratischen Zahlkörpern.* Matematische Nachrichten **21** (1960), 233–284.

[7] M. Eichler, *Zur Zahlentheorie der Quaternionen-Algebren.* J. Reine Angew. Math. **195** (1955), 127–151.
[8] J. G. Huard, B. K. Spearman, K. S. Williams, *Integral Bases for Quartic Fields with Quadratic Subfields.* J. Number Theory **51** (1995), 87–102.
[9] I. Kaplansky, *Submodules of quaternion algebras.* Proc. London Math. Soc. **19** (1969), 219–232.
[10] O. Körner, *Ordnungen von Quaternionalgebren über lokalen Körpern.* J. Reine Angew. Math. **333** (1982), 162–178.
[11] H. W. Lenstra Jr., *Quelques examples d'anneaux euclidiens.* C. R. Acad. Sci. **286** (1978), 683–685.
[12] 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.
[13] J. Neukirch, *Algebraische Zahlentheorie.* Springer-Verlag Berlin Heidelberg, 1992.
[14] M. Peters, *Ternäre und quaternäre quadratische Formen und Quaternionalgebren.* Acta Arith. **15** (1969), 329–365.
[15] H. P. Rehm, *On a Theorem of Gauss Concerning the Number of Integral Solutions of the Equation $x^2 + y^2 + z^2 = m$.* Lecture Notes in Pure and Applied Mathematics Vol. 79, (O. Taussky-Todd, Ed.), Dekker, New York, 1982.
[16] I. Reiner, *Maximal Orders.* Academic Press Inc. (London) Ltd, 1975.
[17] T. R. Shemanske, *Representations of Ternary Quadratic Forms and the Class Number of Imaginary Quadratic Fields.* Pacific J. Math. **122** (1986), 223–250.
[18] T. R. Shemanske, *Ternary Quadratic Forms and Quaternion Algebras.* J. Number Theory **23** (1986), 203–209.
[19] V. Schneider, *Die elliptischen Fixpunkte zu Modulgruppen in Quaternionen-schiefkörpern.* Math. Ann. **217** (1975), 29–45.
[20] B. K. Spearman, K. S. Williams, *Relative integral bases for quartic fields over quadratic subfields.* Acta Math. Hungar. **70 (3)** (1996), 185–192.
[21] M-F. Vignéras, *Arithmétique des Algèbres de Quaternions.* Springer-Verlag Berlin Heidelberg, 1980.

Elise Björkholdt
Department of Mathematics,
Chalmers University of Technology
and Göteborg University,
S-412 96 Göteborg, SWEDEN
*E-mail* : elise@math.chalmers.se