# ON INTEGRAL REPRESENTATIONS BY TOTALLY POSITIVE TERNARY QUADRATIC FORMS

ELISE BJÖRKHOLDT

ABSTRACT. Let $K$ be a totally real algebraic number field such that its 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.

## 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 Hans 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 $N \in R$. He also gave a formula for the number of solutions (see [12]).

In this article, we shall discuss similar results for representations of integers by totally definite ternary quadratic forms with integer coefficients in totally real algebraic number fields.

As an application, we give a proof of Maass' result, based on algebraic methods. Moreover, we prove that there is always a primitive representation of $N$ by $f$ (that is, a solution to $f(x_1, x_2, x_3) = N$ such that $GCD(x_1, x_2, x_3) = 1$). Furthermore, using a result on the stability of embedding numbers of quadratic $R$-orders into quaternion $R$-orders, we find that the number of primitive representations $r_f^0(N)$ of a totally positive non-unit $N \in R$ is given by

1991 *Mathematics Subject Classification.* 11E12, 16H05, 11E20, 11E25, 11E88.

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

where $S = R[\sqrt{-N}]$ and $\gamma_i = 12, 24$ or $32$.

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. After an auxiliary Section 1, we prove in Section 2 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 totally positive constant, which only depends on $f$. In Section 3, we examine the stability of the embedding numbers in a special case. Finally, in Section 4 , we consider the sum of three squares over $R = \mathbb{Z}[\frac{1+\sqrt{5}}{2}]$ and we prove the existence of primitive representations of $N \in R$ by $f$. We also find an explicit formula for the number of such representations.

## 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 $\mathfrak{p}$.

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 [1]).

Two quadratic forms $f$ and $g$ are equivalent over $R$ if there is a linear mapping $\varphi(x_i) = \sum a_{ij}x_j$, with $a_{ij} \in R$, such that $\det[a_{ij}] \in R^*$ and $f(\varphi(x_1),\varphi(x_2),\varphi(x_3)) = g(x_1,x_2,x_3)$. 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 $R$.

## 2. Representations by ternary quadratic forms

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.

**2.1. Proposition.** *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 $x^2 = -c_f N$.*

This is a generalization of Prop. 3.2 in [4] and a proof can be given along the same lines. 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 $V = Ke_1 + Ke_2 + Ke_3$, $q(\sum_{i=1}^3 x_ie_i) = f(x_1,x_2,x_3)$ 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 $\Lambda = C_0(L^\#, c_0q)$ and $c_f = \frac{c_0^2}{2\det(M_f)}$, where $c_0 = \frac{2\det(M_f)}{\Omega_f}$.

Thus, instead of counting representations of $N$ by $f$, we may count solutions to $x^2 = -c_fN$ in $\Lambda$. We will now take this one step further, so that we may look at embeddings of $R[\sqrt{-c_fN}]$ into $\Lambda$ instead of solutions to the equation. For this purpose, we need a relation between quadratic lattices and quaternion orders.

**2.2. Proposition.** *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,*

$$q(x_1f_1 + x_2f_2 + x_3f_3) = d_\Lambda nr(x_1f_1 + x_2f_2 + x_3f_3),$$

*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 $\Lambda \cong C_0(L, q)$.*

*Proof.* We follow the proof of Prop. 3.2 in [1]. Every $R$-lattice in $A$ is free, since $R$ is a principal ideal domain. Let $\Lambda = R + Re_1 + Re_2 + Re_3$. Then $\Lambda^\# = Rf_0 + Rf_1 + Rf_2 + Rf_3$, where $f_0, f_1, f_2, f_3$ is the basis for $A$ over $K$ dual to $1, e_1, e_2, e_3$ with respect to the reduced trace form. Since $tr(f_i) = 0$, for $i = 1, 2, 3$, we get $A_0 = Kf_1 + Kf_2 + Kf_3$. Thus

$$L = A_0 \cap \Lambda^\# = Rf_1 + Rf_2 + Rf_3$$

and

$$nr(r_1f_1 + r_2f_2 + r_3f_3) =$$
$$nr(f_1)r_1^2 + nr(f_2)r_2^2 + nr(f_3)r_3^2 - tr(f_1f_2)r_1r_2 - tr(f_3f_1)r_3r_1 - tr(f_2f_3)r_2r_3.$$

One can easily check that

$$f_if_j = tr(f_if_jf_0) + tr(f_1f_2f_3)e_k, \tag{2.3}$$

$$e_k = tr(f_1f_2f_3)^{-1}(f_if_j - tr(f_if_jf_0)), \tag{2.4}$$

where $(i, j, k)$ is an even permutation of $(1, 2, 3)$.

We know that the element $d = tr((e_1e_2 - e_2e_1)\bar{e_3})$ generates the ideal $d(\Lambda)$, where $x \mapsto \bar{x}$ is the standard anti-involution on $A$ (see [1] Lemma(1.1)). Using (2.4), we get $d = -tr(f_1f_2f_3)^{-1}$. Let $d_\Lambda = tr(f_1f_2f_3)^{-1}$ and denote by $N(\Lambda^\#)$ the ideal generated by all norms $nr(\lambda)$, where $\lambda \in \Lambda^\#$. Then $N(\Lambda^\#)d(\Lambda) \subseteq R$ (see [1], p. 21) , and $N(\Lambda^\#)^{-1}\Lambda^\#\Lambda^\#$ is an $R$-order (see [11], Tum. 6). Since $d(\Lambda)\Lambda^\#\Lambda^\# \subseteq N(\Lambda^\#)^{-1}\Lambda^\#\Lambda^\#$, the products $d_\Lambda f_if_j$ are integral over $R$. Using this fact and (2.3), we get, $d_\Lambda tr(f_if_jf_0) \in R$. Hence

$$\Lambda = R + Rd_\Lambda f_1f_2 + Rd_\Lambda f_3f_1 + Rd_\Lambda f_2f_3.$$

Observe that all products $d_\Lambda f_if_j$, where $i, j \in \{0, 1, 2, 3\}$, are in $\Lambda$. This follows from the equalities

$$f_0^2 = f_0 - nr(f_0),\ f_i^2 = -nr(f_i)\ \text{ for }\ i = 1, 2, 3$$

and

$$f_if_j = \sum_{n=0}^{3} tr(f_if_jf_n)e_n \ \text{ with }\ e_0 = 1.$$

Let $\tilde{E}_i = d_\Lambda f_jf_k$, where $(i, j, k)$ is an even permutation of $(1, 2, 3)$. Let $E_i = f_jf_k$. Then $1, E_1, E_2, E_3$ is a basis for the even Clifford algebra $C_0(L, d_\Lambda nr)$. It is now easy to check that $E_i \mapsto -\tilde{E}_i$ is an isomorphism. □

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 mapping $\varphi : L \to L'$, $\varphi(L) = L'$ and an element $c \in R^*$ such that $q'(\varphi(x)) = cq(x)$ for all $x \in L$. Prop. 2.2 and straightforward calculations will give the following proposition:

**2.5. Proposition.** *There is a one-to-one correspondence 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 $f(x_1,x_2,x_3) = \sum a_{ij}x_ix_j = q(x_1e_1 + x_2e_2 + x_3e_3)$ and let $\Lambda = C_0(L^{\#}, c_0q)$. 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 $A$ the matrix representing $\sigma$ in the basis $e_1, e_2, e_3$. We have $A^tM_qA = cM_q$, so $(\det(A))^2 = c^3$, 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 $\det(A) > 0$ and $-1$ otherwise. Let $\tilde{A}$ be the matrix for $\sigma_{\tilde{c}}$. We have $\sigma_{\tilde{c}}(L) = L$, $\det(\tilde{A}) = 1$ 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 $c_f$.

**2.6. Lemma.** *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 $(L_1^{\#}, c_0q_1), \ldots, (L_t^{\#}, c_0q_t)$ will represent all classes in the genus of $(L^{\#}, c_0q)$. Assume that $\Lambda'$ and $\Lambda = C_0(L^{\#}, c_0q)$ are in the same genus. Then $d(\Lambda) = d(\Lambda')$ and we may choose $d_\Lambda = d_{\Lambda'}$. Using Prop. 2.2, 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 the determinants $\det(M_{q'})$ and $\det(M_{q''})$ can 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 $\Lambda_i$.

□

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.

Let $S_0 = R[\sqrt{-c_fN}]$. 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 $S_0 \subseteq S \subset K(\sqrt{-c_fN})$. We

have $r_f(N) = \sum_S e(S,\Lambda)$, where $e(S,\Lambda)$ denotes the embedding number of $S$ into $\Lambda$, that is, the number of optimal embeddings $S \to \Lambda$.

$\Lambda^*$ acts on the set of embeddings $\varphi : S \to \Lambda$ by inner automorphisms, that is, for $\alpha \in \Lambda^*$, $(\alpha \circ \varphi)(s) = \alpha\varphi(s)\alpha^{-1}$, $s \in S$. The isotropy group for $\varphi$ 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 $[\Lambda^* : S^*]$. Let $e_{\Lambda^*}(S,\Lambda)$ denote the number of $\Lambda^*$-orbits on the set of embeddings of $S$ in $\Lambda$. We know that $[\Lambda^* : S^*] < \infty$ since $[\Lambda^* : R^*] < \infty$, see [9], Satz 2. Thus, we have the equality

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

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

$$\sum_{i=1}^{t} \frac{r_{f_i}(N)}{|\mathrm{Aut}^+(f_i)|} = \sum_{i=1}^{t}\sum_{S} \frac{e(S,\Lambda_i)}{|\mathrm{Aut}(\Lambda_i)|} = \tag{2.8}$$

$$\sum_{i=1}^{t}\sum_{S} \frac{|\Lambda_i^*/R^*|}{|S^*/R^*||\mathrm{Aut}(\Lambda_i)|H(\Lambda_i)} H(\Lambda_i)e_{\Lambda_i^*}(S,\Lambda_i),$$

where $H(\Lambda)$ denotes the order of the group $\mathcal{H}(\Lambda)$, consisting of the locally-free two-sided $\Lambda$-ideals modulo the principal two-sided $\Lambda$-ideals. We will now see that the first factor in this expression does not depend on $i$.

**2.9. Proposition.** *$|\Lambda_i^*/R^*|/H(\Lambda_i)|\mathrm{Aut}(\Lambda_i)|$ is the same for all $i$.*

*Proof.* We follow the proof of Prop. 3.5 in [4]. Let $\mathcal{A}ut(\Lambda) = \{\sigma = (\sigma_\mathfrak{p})_\mathfrak{p}$: $\sigma_\mathfrak{p}(x) = \alpha_\mathfrak{p} x \alpha_\mathfrak{p}^{-1}$, $\alpha = (\alpha_\mathfrak{p})_\mathfrak{p} \in \mathcal{J}(A)$ and $\sigma_\mathfrak{p}(\hat{\Lambda}_\mathfrak{p}) = \hat{\Lambda}_\mathfrak{p}\}$, where $\mathfrak{p} \in SpecR$, $\mathfrak{p} \neq 0$, and $\mathcal{J}(A)$ is the idèle group of $A$. Denote $\sigma = [\alpha]$. Then $[\alpha] = [\beta]$ if and only if $\alpha_\mathfrak{p}^{-1}\beta_\mathfrak{p} \in \hat{K}_\mathfrak{p}^*$ ($[\alpha] = [\beta] \Leftrightarrow \alpha_\mathfrak{p}^{-1}\beta_\mathfrak{p} x = x\alpha_\mathfrak{p}^{-1}\beta_\mathfrak{p}$, where $x \in \hat{\Lambda}_\mathfrak{p} \Leftrightarrow \alpha_\mathfrak{p}^{-1}\beta_\mathfrak{p}$ commutes with all elements of $\hat{A}_\mathfrak{p} \Leftrightarrow \alpha_\mathfrak{p}^{-1}\beta_\mathfrak{p} \in \hat{K}_\mathfrak{p}^*$). Let $\mathcal{A}ut^*(\Lambda)$ be the subgroup of $\mathcal{A}ut(\Lambda)$ consisting of $\sigma = [(\alpha_\mathfrak{p})_\mathfrak{p}]$ such that $\alpha_\mathfrak{p} \in \Lambda^*$. There is a surjective group homomorphism $\varphi : \mathcal{A}ut(\Lambda)/\mathcal{A}ut^*(\Lambda) \to \mathcal{H}(\Lambda)$ such that $\sigma = [\alpha]$ is mapped onto the class of $\Lambda\alpha$. The kernel of this homomorphism will be

$$\frac{\mathcal{A}ut^*(\Lambda)\mathrm{Aut}(\Lambda)}{\mathcal{A}ut^*(\Lambda)} \cong \frac{\mathrm{Aut}(\Lambda)}{\mathrm{Aut}^*(\Lambda)},$$

where $\mathrm{Aut}(\Lambda)$ is the automorphism group of $\Lambda$ and $\mathrm{Aut}^*(\Lambda)$ is the subgroup induced by the elements of $\Lambda^*$. Hence we get

$$|\mathcal{A}ut(\Lambda)/\mathcal{A}ut^*(\Lambda)| = |\mathrm{Aut}(\Lambda)/\mathrm{Aut}^*(\Lambda)|H(\Lambda).$$

Every automorphism of $\Lambda$ can be extended to an automorphism of A, so we know that this is an inner automorphism (by the Skolem-Noether theorem) given by an element $\alpha \in A^*$ and hence $\mathrm{Aut}^*(\Lambda) \cong \Lambda^*/R^*$. We also notice that $|\mathcal{A}ut(\Lambda_i)/\mathcal{A}ut^*(\Lambda_i)|$ remains the same for all orders $\Lambda_i$ in the genus of $\Lambda$. This observation concludes the proof. □

We also need the following proposition from [4], p. 204.

**2.10. Proposition.** *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*

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

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

Interchanging the summation order in (2.8) and applying Prop. 2.9 and 2.10, we get

**2.11. Theorem.** *Let $f$ be a totally positive definite ternary quadratic form and $\Lambda = C_0(L^{\#}, c_0 q)$ the quaternion order corresponding to $f$ according to Prop.* 2.1. *Let $f_1 = f, \ldots, f_t$ 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 make the following observation.

**2.12. Lemma.** *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 a basis, $a_0, a_1, a_2, a_3$, for $\Lambda$ such that $\Lambda = Ra_0 + Ra_1 + Ra_2 + Ra_3$ and $\varphi(S) = Rd_0a_0 + Rd_1a_1$, where $d_0, d_1 \in R$ and $d_0 | d_1$. Then

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

so $\Lambda/\varphi(S)$ 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 $\lambda = r_0 + r_1E_1 + r_2E_2 + r_3E_3$ 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 2.12, we have a Corollary, which gives us a formula for the number of primitive representations of $N$ by $f$ when $t = 1$.

**2.13. Corollary.** *With the same notations as in Prop.* 2.11,

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

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

## 3. Stability of the embedding numbers

We will now obtain a result concerning the stability of the embedding numbers in a special case.

**3.1. Lemma.** *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 denote by $R'$ the integers in $K'$. Then $S \subseteq R'$ is a suborder. By Thm. 12.12 in [13], $rank(S^*) = rank(R'^*)$ and $|R'^*/S^*| < \infty$. Thus $|S^*/R^*| < \infty$, since $|R'^*/R^*| < \infty$. Furthermore, $S^*$ is a fintely generated $\mathbb{Z}$-module, so $S^* \cong T \oplus \mathbb{Z}^k$, for some $k$, where $T$ denotes the torsion elements in $S^*$. Using Dirichlet's unit theorem, we have $R'^* \cong W_{R'} \times \mathbb{Z}$ and $R^* \cong W_R \times \mathbb{Z}$, where $W_{R'}$ and $W_R$ denote the sets of roots of unity in $R'^*$ and in $R^*$ respectively. $R^* \subseteq S^* \subseteq R'^*$, so $S^* \cong W_S \times \mathbb{Z}$. We will now consider possible roots of unity in $S$. We know that $W_R = \{1, -1\}$. Let $\varepsilon_n$ 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 $n = 2, 3, 4, 5, 8, 10, 12$. It is then easy to check that $W_S = W_R$. Now we let $\varepsilon$ denote the fundamental unit in $R$ and let $\varepsilon'$ denote the fundamental unit in $S$. We then have that $(\varepsilon')^k = \varepsilon$ for some $k$ and $Nr_{K'/K}(\varepsilon') \in R^*$. Since $\varepsilon \in \mathbb{R}$ and $S = R + R\sqrt{-\alpha}$, we get $\varepsilon' \in R$, so $\varepsilon' = \varepsilon$. □

Let $\Lambda$ be an $R$-order in a quaternion algebra $A$. We use Prop. 2.2 to find $f(x_1, x_2, x_3,) = \sum_{i,j} a_{ij}x_ix_j$ such that $\Lambda \cong C_0(f)$. Recall the following well-known facts: The $R$-order $\Lambda$ is

$(i)$ hereditary (i.e. every ideal of $\Lambda$ is a projective $\Lambda$-module) if and only if $d(\Lambda)$ is square-free (see [2], Prop. 1.2).

$(ii)$ Gorenstein (i.e. $\Lambda^{\#}$ is projective as a left $\Lambda$-module) if and only if the greatest common divisor for the $a_{ij}$'s is equal to 1 (see [1], Thm. 3.4).

$(iii)$ a Bass order (i.e. each $R$-order $\Lambda'$ such that $\Lambda \subseteq \Lambda' \subseteq A$ is Gorenstein) if and only if each completion $\hat{\Lambda}_{\mathfrak{p}}$ is a Bass order for every prime $\mathfrak{p}$ in $R$ (see [7], p. 778). We also recall that $\Lambda$ is a Bass order if $d(\Lambda)$ is cube-free (see [2], Cor. 1.6).

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 [2], Prop. 1.4).

Let $f$ be such that $G(\Lambda_f)$ is a Bass order, where $\Lambda_f$ is the order corresponding to $f$ according to Prop. 2.1. We then have the following generalization of Thm. 3.4 in [6]:

**3.2. Theorem.** *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 $d \not\equiv 1 \pmod 8$ be such that $R$ is a principal ideal domain. Let*

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

*as in Cor. 2.13, $S = R[\sqrt{-c_f N}]$ 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 squarefree, such that for all $\mathfrak{p} | d(\Lambda_f)$ we have*

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

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

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

*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 $(d_{\Lambda_f}) \cap \mathbb{Z}$, where $d(\Lambda_f) = (d_{\Lambda_f})$.*

*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 $|S^*/R^*| = 1$ 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 [6], 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 $i(\mathfrak{p}) \leq v_\mathfrak{p}(d(\Lambda_f))$. 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 [15] and the classification of possible cases given in [10] 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 $d(\Lambda_f)$ and let $\Lambda$ denote a maximal order in $A$ such that $\Lambda_f \subseteq \Lambda$. Then $\mathfrak{p}$ does not divide $d(\Lambda)$, so $\hat{A}_\mathfrak{p} = A \otimes \hat{K}_\mathfrak{p}$ is split (see e.g. Cor. 5.3 in [16]). Since $\mathfrak{p}$ does not divide $d(\Lambda_f)$, we also know that $\hat{\Lambda}_{f\mathfrak{p}}$ is a maximal order and thereby hereditary ($d(\hat{\Lambda}_{f\mathfrak{p}})$ is square-free). According to Prop. 3.1.(b) in [5], we have $e(\hat{S}_\mathfrak{p}, \hat{\Lambda}_{f\mathfrak{p}}) = 1$.

Let $\mathfrak{p}|d_{\Lambda_f}$. 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 $d(\Lambda_f) \cap \mathbb{Z}$ is possible since $i(\mathfrak{p}) \leq v_\mathfrak{p}(d_{\Lambda_f})$.

□

**3.8. Corollary.** *The notations are 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 $d_{\Lambda_f}$ 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 $d(\Lambda_f) \cap \mathbb{Z}$ 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 [8], Satz 24). We know that $\Lambda_f$ is a Bass order since $d(\Lambda_f) = 4$ is cube-free.

We 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 $\hat{R}_{\mathfrak{p}}$. Let $g$ be a ternary quadratic form such that the even Clifford algebra $C_0(g)$ is isomorphic to $\Lambda$. If $\hat{\Lambda}_{\mathfrak{p}}$ is not a maximal order in a matrix algebra over $K$, then according to [3], (2.6), $|e_{\mathfrak{p}}(\Lambda)| + 1$ is equal to the rank of $g$ modulo $\mathfrak{p}$. Moreover, if $e_{\mathfrak{p}}(\Lambda) = 1$, then $g$ modulo $\mathfrak{p}$ is a product of two different linear factors and if $e_{\mathfrak{p}}(\Lambda) = -1$, then $g$ is irreducible modulo $\mathfrak{p}$.

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 number.

**4.1. Theorem.** *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 infinte 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 [16], Chap. II, Cor. 5.3 and Chap. III, Thm. 3.1). Since $d_\Lambda = 4$, we then know that $A$ only ramifies at the infinite primes. Furthermore, $\hat{\Lambda}_2$ is not maximal, but $\hat{\Lambda}_\mathfrak{p}$ is maximal for all primes $\mathfrak{p} \neq 2$ in $R$.

Using Lemma 2.12 and Cor. 2.13, all we need to show is that for a totally positive integer $N \in R$ it is possible to embedd $S = R[\sqrt{-N}]$ 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 [16], 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.

The rank of $f$ modulo 2 is 1, so $e_2(\Lambda) = 0$. If 2 divides $\Delta(L/K)$, then $e(\hat{S}_2, \hat{\Lambda}_2) \neq 0$, by 3.14 in [5] if $\hat{S}_2$ is maximal in $\hat{L}_2$, since $L$ is ramified over $K$, and by 3.17 in [5] 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 [5], 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 $r_f^0(N) = 6$.

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 [10], Thm. 1 in [15] 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 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

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

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 [14], 3.4). PARI-GP was used for these computations. From our results, we deduce that the only possible values for $\gamma(N)$ are $\frac{1}{2}, 1$ and $\frac{4}{3}$. The values of $r_f^0(N)$ for $N = N_0^2 N_1$ will be

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

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

## References


1. J. Brzezinski, A Characterisation of Gorenstein Orders, Math. Scand. 50 (1982), 19-24.
2. J. Brzezinski, On orders in quaternion algebras, Communications in Algebra, 11(5) (1983), 501-522.
3. J. Brzezinski, Spinor Class Groups of Orders, Journal of Algebra 84, 1983, 468-481.
4. J. Brzezinski, A combinatorial class number formula, J.reine angew. Math. 402, (1989), 199-210.
5. J. Brzezinski, On automorphisms of quaternion orders, J.reine angew. Math. 403, (1990), 166-186.
6. J. Brzezinski, On embedding numbers into quaternion orders, Comment. Math. Helvetici 66 (1991), 302-318.
7. C. W. Curtis and I. Reiner, Methods of representation theory, Vol. I, John Wiley & Sons, Inc., New York, 1981.
8. J. Dzewas, Quadratsummen in reell-quadratischen Zahlörpern, Matematische Nachrichten 21, 1960, 233-284.
9. M. Eichler, Zur Zahlentheorie der Quaternionen-Algebren, J. Reine Angew. Math. 195 (1955), 127-151.
10. J. G. Huard, B. K. Spearman and K. S. Williams, Integral Bases for Quartic Fields with Quadratic Subfields, J. Number Theory 51 (1995), 87-102.
11. I. Kaplansky, Submodules of quaternion algebras, Proc. London Math. Soc. 19, (1969), 219-232.
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. V. Schneider, Die elliptischen Fixpunkte zu Modulgruppen in Quaternionenschiefkörpern, Math. Ann., 217 (1975), 29-45.
15. B. K. Spearman and K. S. Williams, Relative integral bases for quartic fields over quadratic subfields, Acta Math. Hungar. 70 (3) (1996), 185-192.
16. M-F. Vignéras, Arithmétic des Algèbres de Quaternions, Springer-Verlag Berlin Heidelberg, 1980.


Department of Mathematics, Chalmers University of Technology and Göteborg University, S-412 96 Göteborg, Sweden