

Sums of squares in S -integers

Vítězslav Kala and Pavlo Yatsyna

ABSTRACT. In totally real number fields, we characterize the rings of S -integers (obtained by inverting a rational integer m) such that all their totally positive elements are represented as a sum of squares. We further obtain partial answers to the question: when are all the totally positive algebraic integers that are divisible by m represented as a sum of squares?

CONTENTS

1. Introduction	1145
2. Local-global principle	1147
3. Quadratic case	1150
Acknowledgments	1152
References	1153

1. Introduction

In 1921, Siegel [Si1] proved Hilbert’s conjecture that *in any number field K , every totally positive element can be represented as a sum of four squares of elements of K .*

The study of similar questions for rings of integers in number fields turned out to be much subtler. Of course, already in 1770, Lagrange proved that every positive integer is a sum of four squares. In the case of totally real number fields, Maaß and Siegel [Ma, Si2] showed that the only other case when every totally positive integer is a sum of squares (in the ring of integers) is $\mathbb{Q}(\sqrt{5})$. In the non-totally real case, the necessary and sufficient condition for this to happen is that 2 is unramified [Si2]. Overall, the non-totally real case is better understood, and so we do not consider it in this note.

These results were then generalized in two main directions. Let the *Pythagoras number* of a ring R be the smallest positive integer r such that

Received May 18, 2020.

2010 *Mathematics Subject Classification.* 11E25, 11E12, 11R11.

Key words and phrases. number field, totally real, S -integers, sum of squares, Pythagoras number.

The authors were supported by projects PRIMUS/20/SCI/002 (V.K., P.Y.) and UNCE/SCI/022 (V.K.) from Charles University.

every sum of squares in R is also a sum of at most r squares. In 1980, Scharlau [Sch2] showed that Pythagoras numbers of rings of integers in totally real number fields K can be arbitrarily large. He also formulated a question whether these Pythagoras numbers are bounded in the case of bounded degree $[K : \mathbb{Q}]$; the authors of this note recently answered Scharlau's question in the affirmative [KY]. For more results and history see, e.g., the survey by Leep [Le].

The second rich source of generalizations are *universal quadratic forms*, i.e., quadratic forms that represent all totally positive integers. There is a rich literature concerning them, so let us only briefly note that they exist over each totally real number field by the results of [HKK], but can require arbitrarily large numbers of variables [BK, Ka, Ya].

In this short note, we will focus on the intermediate case between number fields and their rings of integers \mathcal{O} , namely, on the rings of S -integers $\mathcal{O}[\frac{1}{m}]$. In such a setting, Collinet [Col] proved in 2016 that in $\mathcal{O}[\frac{1}{2}]$, every totally positive element is a sum of five squares. We will first generalize his result to the case of arbitrary even m .

Throughout the paper, K will be a totally real number field of degree d over \mathbb{Q} with the ring of integers \mathcal{O} ; the subset of totally positive elements is denoted \mathcal{O}^+ .

Theorem 1.1. *Let $m \in \mathbb{N}$, $m > 1$.*

- a) *If m is even or 2 is unramified in \mathcal{O} , then every totally positive element of $\mathcal{O}[\frac{1}{m}]$ is a sum of five squares in $\mathcal{O}[\frac{1}{m}]$.*
- b) *If m is odd and 2 ramifies in \mathcal{O} , then there exist totally positive elements of $\mathcal{O}[\frac{1}{m}]$ that are not sums of squares in $\mathcal{O}[\frac{1}{m}]$.*

One of our tools is the partial local-global principle for integral representations by quadratic forms due to Hsia, Kitaoka, and Kneser [HKK] (although one could instead directly argue via the genus theory used in the proof of their result). Our resulting Theorem 1.1 leaves open the question of what happens for arbitrary rings of S -integers, although perhaps similar methods may also be useful in the general case.

We get the following corollary to Theorem 1.1 and its proof; these two results will be proved as Theorem 2.3 and Corollary 2.4.

Corollary 1.2. *There exists $m_0 \in \mathbb{N}$ (depending on K) such that for all $m \geq m_0$, every element of $2m\mathcal{O}^+$ is a sum of five squares of elements of \mathcal{O} .*

When 2 is unramified in K , then one does not need to consider only even multiples and gets that each element of $m\mathcal{O}^+$ is a sum of five squares of elements of \mathcal{O} if m is sufficiently large.

The corollary is a significant improvement on the result of Siegel [Si1, Satz 9] which showed that there exists $m \in \mathbb{N}$, depending on K , such that any totally positive integer $\alpha \in \mathcal{O}^+$ can be represented as $\sum \left(\frac{\beta_i}{m}\right)^2$. Specifically,

the number of squares required by Siegel depended on α , i.e., $\frac{m^2 \text{Tr}(\alpha)}{d}$ squares were needed.

We further focus in detail on the case of real quadratic fields $\mathbb{Q}(\sqrt{D})$ in Section 3.

Scharlau [Sch1] showed that in $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{3})$, all the elements of \mathcal{O} that meet local criteria are represented as a sum of squares in \mathcal{O} . This implies that all elements of $2\mathcal{O}^+$ are represented as a sum of squares (of elements of \mathcal{O}), i.e., that one can take $m_0 = 1$. As Theorem 3.1, we prove the converse to his result:

Theorem 1.3. *Let $K = \mathbb{Q}(\sqrt{D})$ with $D \geq 2$ squarefree. Then every element of $2\mathcal{O}^+$ is a sum of squares in \mathcal{O} if and only if $D = 2, 3$, or 5 .*

The Pythagoras number of the ring of integers \mathcal{O} in a real quadratic field is at most 5 [Pet, Satz 2], so every sum of squares in \mathcal{O} is also a sum of at most five squares. In fact, when $D = 2, 3, 5$, the Pythagoras number is 3 [Sch1, Bemerkung 1], and so three squares suffice in these cases.

For the proof, we consider the representability of 2α for a specific element α (motivated by the study of indecomposable elements [DS, HK]).

It is natural to ask whether for given $m \in \mathbb{N}$ there are only finitely many totally real number fields for which every element of $m\mathcal{O}^+$ is a sum of squares in \mathcal{O} . At least for real quadratic fields, we can give the following bounds on m (proved as Theorem 3.2):

Theorem 1.4. *Let $K = \mathbb{Q}(\sqrt{D})$ with $D \geq 2$ squarefree. Let $\kappa = 1$ if $D \equiv 1 \pmod{4}$ and $\kappa = 2$ if $D \equiv 2, 3 \pmod{4}$.*

- a) *If $m < \frac{\kappa\sqrt{D}}{4}$, then not all elements of $m\mathcal{O}^+$ are represented as a sum of squares in \mathcal{O} .*
- b) *If $m \geq \frac{D}{2}$, then all elements of $\kappa m\mathcal{O}^+$ are sums of five squares in \mathcal{O} .*
- c) *If m is odd and $D \equiv 2, 3 \pmod{4}$, then there exist elements of $m\mathcal{O}^+$ that are not sums of squares in \mathcal{O} .*

2. Local-global principle

Let K be a totally real number field of degree $d = [K : \mathbb{Q}]$ with the ring of integers $\mathcal{O} = \mathcal{O}_K$, i.e., K has d real embeddings $\sigma : K \hookrightarrow \mathbb{R}$. An element $\alpha \in K$ is *totally positive* ($\alpha \succ 0$) if $\sigma(\alpha) > 0$ for all σ . For $A \subset K$, we will denote by A^+ the subset of totally positive elements of A . The norm and trace from K to \mathbb{Q} are denoted by N and Tr , respectively.

Some of our arguments will be formulated in the language of quadratic lattices. Let F be a number field or its completion; if $F \neq \mathbb{R}, \mathbb{C}$, then let \mathcal{O}_F be its ring of integers. A *quadratic space over F* is an r -dimensional F -vector space V equipped with a symmetric bilinear form $B : V \times V \rightarrow F$ and the associated quadratic form $Q(v) = B(v, v)$. A *quadratic \mathcal{O}_F -lattice* $L \subset V$ is a finitely generated \mathcal{O}_F -submodule such that $FL = V$; L is equipped with

the restricted quadratic form Q , and so we often talk about a quadratic \mathcal{O}_F -lattice as the pair (L, Q) .

We will only work with the sum of squares quadratic form $Q = x_1^2 + \cdots + x_r^2$ and its associated quadratic \mathcal{O}_F -lattice (\mathcal{O}_F^r, Q) . This lattice is always *unimodular*, i.e., its *dual* $L^\# = \{v \in V \mid B(v, w) \in \mathcal{O}_F \text{ for all } w \in L\}$ equals the lattice L .

An element α is *represented* by the \mathcal{O}_F -lattice L (or by the F -quadratic space V) if there is $v \in L$ (or $v \in V$) such that $Q(v) = \alpha$.

We denote by $\mathfrak{s}L$ the *scale* of a lattice L , i.e., $\mathfrak{s}L = \{\sum B(v_i, w_i) \mid v_i, w_i \in L\}$. Clearly, $\mathfrak{s}L$ is an ideal in \mathcal{O}_F . Let us denote by $Q(L) = \{Q(v) \mid v \in L\}$ the set of all elements represented by Q .

We shall use the partial local-global principle by Hsia, Kitaoka, and Kneser that we formulate only for a sum of squares, as this is the case we need.

Theorem 2.1 ([HKK, Theorem 3]). *There exists a constant $C = C(K)$ such that, for every $\alpha \in \mathcal{O}^+$ with $N(\alpha) \geq C$, we have that α is represented as a sum of five squares in \mathcal{O} if and only if α is represented everywhere locally as a sum of five squares.*

To be precise, we say that α is *represented everywhere locally* if it is represented over all the archimedean completions of K and over the rings of integers \mathcal{O}_F in all the non-archimedean completions F . Similarly, when we, e.g., say *over all the completions at dyadic primes*, we mean over the rings of integers \mathcal{O}_F in all the completions F of K at prime ideals $\mathfrak{p} \mid 2\mathcal{O}$.

The next lemma is a known result (see for example [BDS, Remark 1]), but we could not find its proof in the literature, so we reprove it for the benefit of the reader.

Lemma 2.2. *Let $\alpha \in \mathcal{O}$ and $r \in \mathbb{N}, r \geq 5$. Then α is a sum of r squares over all the completions at dyadic primes if and only if α is a square modulo $2\mathcal{O}$.*

Proof. Let $2\mathcal{O} = \prod_{i=1}^k \mathfrak{p}_i^{e_i}$ where \mathfrak{p}_i are pairwise distinct prime ideals. We have $x_1^2 + \cdots + x_r^2 \equiv (x_1 + \cdots + x_r)^2 \pmod{\mathfrak{p}_i^{e_i}}$, i.e., any sum of squares is congruent to a square modulo $\mathfrak{p}_i^{e_i} \mid 2\mathcal{O}$. Thus, if α is represented as a sum of squares over the completion at \mathfrak{p}_i , then α is congruent to a square modulo $\mathfrak{p}_i^{e_i}$. The Chinese Remainder Theorem then implies that α is congruent to a square also modulo $2\mathcal{O}$, as needed.

Now assume that $\alpha \equiv \beta^2 \pmod{2\mathcal{O}}$, i.e., $\alpha = \beta^2 + 2\delta$ for some $\delta \in \mathcal{O}$. Consider a prime ideal $\mathfrak{p} \mid 2\mathcal{O}$ and let F be the corresponding completion of K . Let L be the \mathcal{O}_F -lattice associated to the quadratic form $Q(x) = x_1^2 + \cdots + x_r^2$. This sum of squares lattice is unimodular and the rank of L is $r \geq 5$, and so by [OMe, 93:18(v)] (that uses the assumption that we are working dyadically), we deduce that $Q(L) = Q(L) + 2(\mathfrak{s}L)$. At

the same time, as Q represents 1, we have $\mathfrak{s}L = \mathcal{O}$, and so $\delta \in \mathfrak{s}L$ and $\alpha = \beta^2 + 2\delta \in Q(L) + 2(\mathfrak{s}L) = Q(L)$, as needed. \square

We can now prove our first theorem and corollary.

Theorem 2.3. *Let $m \in \mathbb{N}$, $m > 1$.*

- a) *If m is even or 2 is unramified in \mathcal{O} , then every totally positive element of $\mathcal{O} \left[\frac{1}{m} \right]$ is a sum of five squares in $\mathcal{O} \left[\frac{1}{m} \right]$.*
- b) *If m is odd and 2 ramifies in \mathcal{O} , then there exist totally positive elements of $\mathcal{O} \left[\frac{1}{m} \right]$ that are not sums of squares in $\mathcal{O} \left[\frac{1}{m} \right]$.*

Proof. a) Let us consider a totally positive element of $\mathcal{O} \left[\frac{1}{m} \right]$ and write it as $\frac{\alpha}{m^k}$, where $\alpha \in \mathcal{O}$ and $k \in \mathbb{Z}$. By multiplying the numerator and denominator of $\frac{\alpha}{m^k}$ by a sufficiently large power of m , we can without loss of generality assume that α satisfies the norm assumption in Theorem 2.1 and that k is even. Thus, to apply this theorem, we need to show that α is represented everywhere locally as a sum of five squares. This is clear over all archimedean places, as α is totally positive.

Over every non-dyadic prime, every unimodular lattice of rank ≥ 3 is universal [OMe, 92:1b], and thus α is a sum of 3 squares (in the considered non-dyadic completion of K), and *a fortiori* of 5 squares.

For a dyadic prime $\mathfrak{p} \mid 2\mathcal{O}$, by Lemma 2.2, α is a sum of five squares if and only if α is a square modulo $2\mathcal{O}$. If m is even, then we can without loss of generality replace $\frac{\alpha}{m^k}$ by $\frac{m^2\alpha}{m^{k+2}}$ so that $\alpha \equiv 0 \equiv 0^2 \pmod{2\mathcal{O}}$. If 2 is unramified in \mathcal{O} , then $\mathcal{O}/2\mathcal{O}$ is a product of fields of characteristic 2, and hence every element of \mathcal{O} is a square modulo $2\mathcal{O}$.

b) Assume that m is odd and 2 ramifies, i.e., $2\mathcal{O} = \prod_{i=1}^k \mathfrak{p}_i^{e_i}$, where \mathfrak{p}_i are pairwise distinct primes and at least one $e_i > 1$; assume that $e_1 > 1$. Choose an element $\alpha_0 \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$ and add to it a sufficiently large even rational integer, $2a$, so that the sum $\alpha = \alpha_0 + 2a \in \mathfrak{p}_1 \setminus \mathfrak{p}_1^2$ is totally positive; assume for contradiction that α is a sum of squares in $\mathcal{O} \left[\frac{1}{m} \right]$.

As m is odd, it is invertible modulo $\mathfrak{p}_1^{e_1}$, and so α is congruent to a sum of squares in $\mathcal{O}/\mathfrak{p}_1^{e_1}$. As in the second line of the proof of Lemma 2.2, this implies that $\alpha \equiv \beta^2 \pmod{\mathfrak{p}_1^{e_1}}$ for some $\beta \in \mathcal{O}$. We have $\alpha \in \mathfrak{p}_1$, and so $\beta^2 \in \mathfrak{p}_1$. Therefore, $\beta \in \mathfrak{p}_1$ (for \mathfrak{p}_1 is a prime ideal), and finally $\alpha \in \mathfrak{p}_1^2$, a contradiction. \square

Corollary 2.4. *There exists $m_0 \in \mathbb{N}$ (depending on K) such that for all $m \geq m_0$, every element of $2m\mathcal{O}^+$ is a sum of five squares of elements of \mathcal{O} .*

Proof. Let $2m \geq C^{1/d}$ where C is the constant from Theorem 2.1 and consider $\alpha \in \mathcal{O}^+$. We need to show that $2m\alpha$ can be represented as a sum of five squares in \mathcal{O} .

We have $N(2m\alpha) \geq (2m)^d \geq C$, and so the norm condition from Theorem 2.1 is satisfied for $2m\alpha$.

Further, $2 \mid 2m\alpha$, and so the element $2m\alpha$ is represented everywhere locally as we saw in the proof of Theorem 2.3. Thus, $2m\alpha$ is a sum of five squares by Theorem 2.1. \square

In the case when m is odd and 2 ramifies, one can argue analogously using Theorem 2.1 (and the observation that a sum of squares always satisfies the local conditions at dyadic primes) to show that the Pythagoras number of $\mathcal{O}[\frac{1}{m}]$ is at most 5.

3. Quadratic case

To prove Theorem 1.3, we will need to work with specific elements of K . Throughout this section, we use the following notation. We fix a squarefree integer $D \geq 2$ and consider the real quadratic field $K = \mathbb{Q}(\sqrt{D})$ and its ring of integers \mathcal{O} . Then $\{1, \omega_D\}$ forms an integral basis of \mathcal{O} , where

$$\omega_D = \begin{cases} \sqrt{D} & \text{if } D \equiv 2, 3 \pmod{4}, \\ \frac{1+\sqrt{D}}{2} & \text{if } D \equiv 1 \pmod{4}. \end{cases}$$

The conjugate of $\alpha \in K$ is α' .

Theorem 3.1. *Let $K = \mathbb{Q}(\sqrt{D})$ with $D \geq 2$ squarefree. Then every element of $2\mathcal{O}^+$ is a sum of squares in \mathcal{O} if and only if $D = 2, 3$, or 5.*

Proof. “ \Rightarrow ” Assume that every element of $2\mathcal{O}^+$ is a sum of squares.

Let us start with the case $D \equiv 2, 3 \pmod{4}$.

For the element $\alpha = k + \sqrt{D} \in \mathcal{O}^+$ with $k = \lfloor \sqrt{D} \rfloor + 1$, let $2\alpha = \sum_i \alpha_i^2$ be the corresponding decomposition with $\alpha_i = a_i + b_i\sqrt{D}$, where we can without loss of generality assume that $a_i \geq 0$. We have

$$\alpha_i^2 = a_i^2 + Db_i^2 + 2a_ib_i\sqrt{D}.$$

If $a_i = 0$, then let us also without loss of generality assume that $b_i > 0$.

If for some i we have $a_i > 0$ and $b_i < 0$, then $2\alpha' \geq (\alpha'_i)^2 = a_i^2 + Db_i^2 + 2a_i(-b_i)\sqrt{D} \geq 1 + D + 2\sqrt{D} > 2$, a contradiction, as $\alpha' < 1$. Thus all $b_i \geq 0$.

Comparing irrational parts in the expression for 2α , we see that $1 = \sum_i a_ib_i$. All the summands are non-negative, and so there is exactly one index j with $a_jb_j = 1$ and $a_ib_i = 0$ for all $i \neq j$. Without loss of generality, let $j = 1$ so that $a_1 = b_1 = 1$.

Subtracting α_1^2 from the representation of 2α , we then get $2k - (1 + D) = \sum_{i \geq 2} \alpha_i^2 \geq 0$, and so

$$2\sqrt{D} + 2 > 2k \geq 1 + D.$$

This is possible only for $D < 6$ (i.e., $D = 2, 3$), finishing this part of the proof.

Let us now take $D \equiv 1 \pmod{4}$ and $\alpha = k + \omega_D = (k + 1/2) + \sqrt{D}/2 \in \mathcal{O}^+$ with $k = \lfloor \omega_D \rfloor$. Again, let $2\alpha = \sum_i \alpha_i^2$ with $\alpha_i = a_i + b_i\sqrt{D}$ and $a_i \geq 0$, except this time $a_i = c_i/2, b_i = d_i/2$ can be half-integers (with $2 \mid c_i - d_i$ for

all i). Nevertheless, as before we have $\alpha' < 1$, from which we deduce that $b_i \geq 0$ for all i .

Comparing coefficients, we then have $1/2 = \sum_i a_i b_i$, and so (without loss of generality) the only possibility is $\alpha_1 = \alpha_2 = \omega_D$ and $a_i b_i = 0$ for all $i > 2$. Then $2k + 1/2 - D/2 = 2\alpha - 2\omega_D^2 = \sum_{i \geq 3} \alpha_i^2 \geq 0$. Thus,

$$2\sqrt{D} + 3 \geq D,$$

which is not possible for $D > 9$. Thus, $D = 5$ in this case.

“ \Leftarrow ” When $D = 5$, Maaß [Ma] showed that every element of \mathcal{O}^+ is a sum of three squares.

When $D = 2, 3$, Scharlau [Sch1] in fact proved that each element that is congruent to a square modulo $2\mathcal{O}$ is a sum of squares. In particular, all elements of $2\mathcal{O}^+$ are sums of squares. \square

Although we did not need this explicitly in the proof, its idea is based on the study of indecomposable integers. We say that $\alpha \in \mathcal{O}^+$ is *indecomposable* if it can not be written as a sum of two totally positive integers. These elements can be explicitly characterized in terms of the periodic continued fraction for ω_D [DS]; our proof was motivated by the study of the possible decompositions of 2α [HK].

Note that it should be possible to use a similar method based on explicitly studying representations of multiples of indecomposables to determine all the real quadratic fields where all elements of $3\mathcal{O}^+$ (or $4\mathcal{O}^+$ or $m\mathcal{O}^+$ for other fixed m) are sums of squares. However, the technical difficulty quickly increases with m . Nevertheless, we at least get

Theorem 3.2. *Let $K = \mathbb{Q}(\sqrt{D})$ with $D \geq 2$ squarefree. Let $\kappa = 1$ if $D \equiv 1 \pmod{4}$ and $\kappa = 2$ if $D \equiv 2, 3 \pmod{4}$.*

- a) *If $m < \frac{\kappa\sqrt{D}}{4}$, then not all elements of $m\mathcal{O}^+$ are represented as a sum of squares in \mathcal{O} .*
- b) *If $m \geq \frac{D}{2}$, then all elements of $\kappa m\mathcal{O}^+$ are sums of five squares in \mathcal{O} .*
- c) *If m is odd and $D \equiv 2, 3 \pmod{4}$, then there exist elements of $m\mathcal{O}^+$ that are not sums of squares in \mathcal{O} .*

Proof. a) The argument is similar to the proof of Theorem 3.1, so let us skip some details.

If $D \equiv 2, 3 \pmod{4}$, let $\alpha = k + \sqrt{D}$ (with $k = \lfloor \sqrt{D} \rfloor + 1$) be the same element as in the proof of Theorem 3.1 and let $m\alpha = \sum_i (a_i + b_i\sqrt{D})^2$ with $a_i, b_i \in \mathbb{Z}$. As before, we obtain that $a_i \geq 0, b_i \geq 0$ for all i (using the upper bound on m).

Comparing irrational parts in the expression for $m\alpha$, we see that $m = 2\sum_i a_i b_i$, and so for some j we have $a_j, b_j \geq 1$. Then $m(2\sqrt{D} + 1) > m\alpha \geq (a_j + b_j\sqrt{D})^2 \geq (1 + \sqrt{D})^2$, which gives a contradiction with $m < \frac{\sqrt{D}}{2}$.

If $D \equiv 1 \pmod{4}$, we consider the element $\alpha = k + \omega_D$ with $k = \lfloor \omega_D \rfloor$. If $m\alpha = \sum_i (a_i + b_i\sqrt{D})^2$ with $a_i, b_i \in \mathbb{Z}/2$, then again $a_i \geq 0, b_i \geq 0$ for all

i , and so $a_j, b_j \geq 1/2$ for some j . This finally implies $m(\sqrt{D} + 1) > m\alpha \geq (a_j + b_j\sqrt{D})^2 \geq (1/2 + \sqrt{D}/2)^2$, which is again impossible.

b) The proof will use a result of Peters [Pet, Satz 2]. To state it, assume first that $D \equiv 1 \pmod{4}$. Given $\alpha \in \mathcal{O}^+$ of the form $\alpha = a_0 + a_1\omega_D$, Peters' theorem states that α is a sum of five squares if and only if there exists a rational integer n in the interval

$$\left[\frac{1}{D} \left(2a_0 + a_1 - 2\sqrt{N(\alpha)} \right), \frac{1}{D} \left(2a_0 + a_1 + 2\sqrt{N(\alpha)} \right) \right]$$

such that $n \equiv a_1 \pmod{2}$.

If the length of this closed interval is at least 2, then it contains at least two consecutive integers, one of which will satisfy the requirement modulo 2. Therefore, if

$$2\sqrt{N(\alpha)} \geq D,$$

then α is represented as a sum of five squares.

Every element $\alpha = m\beta$ with $\beta \in \mathcal{O}^+$ and $m \geq D/2$ satisfies the norm inequality above.

In the case of $D \equiv 2, 3 \pmod{4}$, let $\alpha = a_0 + 2a_1\sqrt{D}$. Then by the same result of Peters, α is a sum of five squares if there exists a rational integer n in

$$\left[\frac{1}{2D} \left(a_0 - \sqrt{N(\alpha)} \right), \frac{1}{2D} \left(a_0 + \sqrt{N(\alpha)} \right) \right].$$

The length of this interval is at least 1 when $\alpha = 2m\beta$ with $\beta \in \mathcal{O}^+$ and $m \geq \frac{D}{2}$, and the coefficient of $\alpha = 2m\beta$ at \sqrt{D} is obviously even as required.

c) Let $D \equiv 2, 3 \pmod{4}$ and consider the element $\alpha = k + \sqrt{D}$ from part a). If $m\alpha$ is a sum of squares as in part a), then $m = 2\sum_i a_i b_i$ is even. \square

Obviously, the argument in part a) and the bound on m can be somewhat improved by considering also the other summands $(a_i + b_i\sqrt{D})^2$.

At least at present, this method is only limited to the quadratic case, as in higher degrees we lack the necessary understanding of indecomposables.

Note that when $D \equiv 1 \pmod{4}$, then Peters' result immediately implies that every element $\alpha \in \mathcal{O}^+$ of norm $> D/2$ is represented as a sum of five squares. E.g., when $D = 5$, then all totally positive units are squares and the smallest norm of a non-unit is $3 > 5/2$, and so this implies that all elements of \mathcal{O}^+ are sums of squares.

Acknowledgments

We thank the anonymous referee for a very careful and fast reading of the manuscript, and for a number of detailed comments that helped to fix some issues and to improve the readability of the article. We also thank Martin Raška for pointing out an error in part b) of Theorem 1.4.

References

- [Bh] BHARGAVA, MANJUL. On the Conway–Schneeberger fifteen theorem. *Quadratic forms and their applications* (Dublin, 1999), 27–37, Contemp. Math., 272, Amer. Math. Soc., Providence, RI, 2000. MR1803359 (2001m:11050), Zbl 0987.11027, doi:10.1090/conm/272.
- [BK] BLOMER, VALENTIN; KALA, VÍTĚZSLAV. Number fields without n -ary universal quadratic forms. *Math. Proc. Cambridge Philos. Soc.* **159** (2015), no. 2, 239–252. MR3395370, Zbl 1371.11084, arXiv:1503.05736, doi:10.1017/S030500411500033X. 1146
- [BDS] BRÖCKER LUDWIG; DRESS ANDREAS; SCHARLAU RUDOLF. An (almost trivial) local-global principle for the representation of -1 as a sum of squares in an arbitrary commutative ring. *Ordered fields and real algebraic geometry* (San Francisco, Calif. 1981), 99–106, Contemp. Math., 8, Amer. Math. Soc., Providence, R.I., 1982. MR0653177 (83k:10039), Zbl 0506.13014, doi:10.1090/conm/008. 1148
- [Col] COLLINET, GAËL. Sums of squares in rings of integers with 2 inverted. *Acta Arith.* **173** (2016), no. 4, 383–390. MR3512861, Zbl 1346.11032, doi:10.4064/aa8363-2-2016. 1146
- [DS] DRESS, ANDREAS; SCHARLAU, RUDOLF. Indecomposable totally positive numbers in real quadratic orders. *J. Number Theory* **14** (1982), no. 3, 292–306. MR0660374 (84a:12005), Zbl 0507.12002, doi:10.1016/0022-314X(82)90064-6. 1147, 1151
- [HK] HEJDA, TOMÁŠ; KALA, VÍTĚZSLAV. Additive structure of totally positive quadratic integers. *Manuscripta Math.* **163** (2020), no. 1-2, 263–278. MR4131999, Zbl 07233351, arXiv:1706.09178, doi:10.1007/s00229-019-01143-8. 1147, 1151
- [HKK] HSIA, JOHN S.; KITAOKA, YOSHIYUKI; KNESER, MARTIN. Representations of positive definite quadratic forms. *J. Reine Angew. Math.* **301** (1978), 132–141. MR560499 (58 #27758), Zbl 0374.10013, doi:10.1515/crll.1978.301.132. 1146, 1148
- [Ka] KALA, VÍTĚZSLAV. Universal quadratic forms and elements of small norm in real quadratic fields. *Bull. Aust. Math. Soc.* **94** (2016), no. 1, 7–14. MR3539315, Zbl 1345.11025, arXiv:1507.04237, doi:10.1017/S0004972715001495. 1146
- [KY] KALA, VÍTĚZSLAV; YATSYNA, PAVLO. Lifting problem for universal quadratic forms. Preprint, 2020. arXiv:1808.02262. 1146
- [Le] LEEP, DAVID B. A historical view of the Pythagoras numbers of fields. *Quadratic forms – algebra, arithmetic, and geometry*, 271–288, Contemp. Math. 493, Amer. Math. Soc., Providence, R.I., 2009. MR2537106 (2010i:11042), Zbl 1229.11060, doi:10.1090/conm/493/09674. 1146
- [Ma] MAASS, HANS. Über die Darstellung total positiver Zahlen des Körpers $R(\sqrt{5})$ als Summe von drei Quadraten. *Abh. Math. Sem. Hansischen Univ.* **14** (1941), 185–191. MR0005505 (3,163a), Zbl 0025.01602, doi:10.1007/BF02940744. 1145, 1151
- [OMe] O’MEARA, O. TIMOTHY. Introduction to quadratic forms. Reprint of the 1973 edition. Classics in Mathematics. Springer-Verlag, Berlin, 2000. xiv+342 pp. ISBN: 3-540-66564-1. MR1754311 (2000m:11032), Zbl 1034.11003, doi:10.1007/978-3-642-62031-7. 1148, 1149
- [Pet] PETERS, MEINHARD. Quadratische Formen über Zahlringen. *Acta Arith.* **24** (1973), 157–164. MR340176 (49 #4932), Zbl 0237.12004, doi:10.4064/aa-24-2-157-164. 1147, 1152
- [Sch1] SCHARLAU, RUDOLF. Darstellbarkeit von ganzen Zahlen durch Quadratsummen in einigen totalreellen Zahlkörpern. *Math. Ann.* **249** (1980), no. 1, 49–54. MR575447 (81m:10034), Zbl 0414.12007, doi:10.1007/BF01387079. 1147, 1151

- [Sch2] SCHARLAU, RUDOLF. On the Pythagoras number of orders in totally real number fields. *J. Reine Angew. Math.* **316** (1980), 208–210. MR581331 (81g:10036), Zbl 0421.12017, doi:10.1515/crll.1980.316.208. 1146
- [Si1] SIEGEL, CARL L. Darstellung total positiver Zahlen durch Quadrate. *Math. Z.* **11** (1921), no. 3-4, 246–275. MR1544496, Zbl 48.0179.04, doi:10.1007/BF01203627. 1145, 1146
- [Si2] SIEGEL, CARL L. Sums of m th powers of algebraic integers. *Ann. of Math. (2)* **46** (1945), 313–339. MR0012630 (7,49b), Zbl 0063.07010, doi:10.2307/1969026. 1145
- [Ya] YATSYNA, PAVLO. A lower bound for the rank of a universal quadratic form with integer coefficients in a totally real number field. *Comment. Math. Helv.* **94** (2019), no. 2, 221–239. MR3942784, Zbl 07067148, arXiv:1808.01441, doi:10.4171/CMH/459. 1146

(Vítězslav Kala) CHARLES UNIVERSITY, FACULTY OF MATHEMATICS AND PHYSICS, DEPARTMENT OF ALGEBRA, SOKOLOVSKÁ 83, 18600 PRAHA 8, CZECH REPUBLIC
`kala@karlin.mff.cuni.cz`

(Pavlo Yatsyna) CHARLES UNIVERSITY, FACULTY OF MATHEMATICS AND PHYSICS, DEPARTMENT OF ALGEBRA, SOKOLOVSKÁ 83, 18600 PRAHA 8, CZECH REPUBLIC
`yatsyna@karlin.mff.cuni.cz`

This paper is available via <http://nyjm.albany.edu/j/2020/26-47.html>.