FACULTY
OF MATHEMATICS
AND PHYSICS
Charles University

BACHELOR THESIS

Martin Raška

Sums of squares in number fields

Department of Algebra

Supervisor of the bachelor thesis: Mgr. Vítězslav Kala, Ph. D.
Study programme: Mathematics
Study branch: General Mathematics

Prague 2021

I declare that I carried out this bachelor thesis independently, and only with the cited sources, literature and other professional sources. It has not been used to obtain another or the same degree.

I understand that my work relates to the rights and obligations under the Act No. 121/2000 Sb., the Copyright Act, as amended, in particular the fact that the Charles University has the right to conclude a license agreement on the use of this work as a school work pursuant to Section 60 subsection 1 of the Copyright Act.

In .... date ....

Author’s signature

I would like to thank very much my supervisor Víťa Kala for introducing me to this engaging topic and for overall great guidance and patience on this project. Thanks are also extended to Danil Koževnikov for useful tips and comments.

Title: Sums of squares in number fields

Author: Martin Raška

Department: Department of Algebra

Supervisor: Mgr. Vítězslav Kala, Ph. D., Department of Algebra

Abstract: The goal of this thesis is to study real quadratic number fields $\mathbb{Q}(\sqrt{D})$ such that, for a given rational integer m, all m-multiples of totally positive integers are sums of squares. We prove quite sharp necessary and sufficient conditions for this to happen. Further, we give a fast algorithm that verifies this property for specific m, D and that for a fixed m finds all such fields in polynomial time.

Keywords: quadratic fields, sum of squares, indecomposables

Contents

Introduction

Throughout history, sums of squares were often in the focus of mathematicians. For number fields, the main question was resolved by Siegel [Si1] in 1921, when he proved Hilbert's conjecture that in every number field, every totally positive number can be represented as the sum of four square elements of the field.

For rings of integers in number fields, we have the well-known result by Lagrange (1770) that every positive rational integer is the sum of four squares. The fact that all totally positive integers can be represented as the sum of squares was later shown to be quite exceptional. While Maaß [Ma] showed that it is also true for $\mathbb{Q}(\sqrt{5})$, Siegel [Si2] proved that $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{5})$ are the only totally positive number fields where this can hold.

The focus of this thesis is on quadratic fields $\mathbb{Q}(\sqrt{D})$ and their totally positive integers $\mathcal{O}^+$. In 1973, Peters [Pet] proved that the *Pythagoras number* of rings of integers R in quadratic fields is at most 5, meaning by definition that an element of R is the sum of any number of squares in R if and only if it is the sum of 5 squares in R. For $D \leq 7$, the Pythagoras number is even smaller, e.g. 3 for $D \in \{2, 3, 5\}$. Summary of these result can be found in [KRS, Sec. 3], where the authors also study a similar question in biquadratic fields. Considering the simplest cubic fields, Tinková [Ti] showed Pythagoras number to be often 6.

However, as we mentioned above, in quadratic fields, all elements of $\mathcal{O}^+$ are sums of squares only for $D = 5$. The natural continuation is further question when all elements of $m\mathcal{O}^+$ (i.e. all m-multiples of totally positive integers) can be represented as the sum of squares for a fixed positive rational integer m. Recently, Kala and Yatsyna [KY] proved that every element of $2\mathcal{O}^+$ is the sum of squares if and only if $D \in \{2, 3, 5\}$. In the general case $m\mathcal{O}^+$, they obtained the following theorem, which gives necessary and sufficient bounds for this to happen.

Theorem 1. [KY, Theorem 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 the 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 $\mathcal{O}$.*

This thesis improves these results for general m. In Chapter 2, the main goal is to further restrict the possibilities for D in terms of m, which results in the following theorem:

Theorem 2. *Let $K = \mathbb{Q}(\sqrt{D})$ with $D \geq 2$ squarefree and m positive integer. If $\sqrt{D}$ lies in one of the following intervals, then* not *all elements of $m\mathcal{O}^+$ can be represented as the sum of squares:*

(a) $\left[\frac{m}{2} + 4, \infty\right)$, $\left[\frac{m}{2i} + i\sqrt{40}, \frac{m}{2(i-1)} - (i-1)\sqrt{70}\right]$ *for integer $i > 1$ and $D \equiv 2, 3 \pmod 4$,*

(b) $\left[\frac{m}{2} + 8, \infty\right)$, $\left[\frac{m}{2i} + 2i\sqrt{40}, \frac{m}{2(i-1)} - 2(i-1)\sqrt{70}\right]$ *for integer $i > 1$, $D \equiv 1 \pmod 4$ and even m,*

(c) $[m + 4, \infty)$, $\left[\frac{m}{2i+1} + (4i+2)\sqrt{40}, \frac{m}{2i-1} - (4i-2)\sqrt{70}\right]$ *for integer $i > 0$, $D \equiv 1 \pmod 4$ and odd m.*

It should be noted that for fixed m, only finitely many of these intervals are non-empty (for further details, see Chapter 2). This not only improves the necessary upper bounds given by Theorem 1 but also gives better insight into the overall structure of the problem.

At the beginning of Chapter 3, we present a proof of Theorem 7 by Peters, which will prove useful in Chapters 3, 4 and 5. These, on the other hand, focus on proving that for specific fields, all elements of $m\mathcal{O}^+$ are sums of squares in $\mathcal{O}$. For example, Theorem 9 gives a detailed proof that all elements of $4\mathcal{O}^+$ are sums of squares if and only if $D \in \{2, 3, 5, 6, 7, 10, 11, 13\}$.

Conversely, if D is of the form of $t^2 - 1$ or $(2t+1)^2 - 4$, Theorems 10 and 11 provide a full characterization of all m that satisfy the given condition. One could give similar results for D in other quadratic families.

In Chapter 5, we provide a general algorithm that completely determines all of these fields satisfying this property for arbitrary m. The algorithm uses the structure of indecomposable elements of $\mathcal{O}^+$ and, for fixed m and D, it proves the statement or finds a counterexample with time complexity $O(\sqrt{D}(\log(D))^2)$. The time complexity for finding all such D for a fixed m turns out to be $O(m^2(\log(m))^3)$. An implementation of this algorithm is available at `https://github.com/raskama/number-theory/tree/main/quadratic`. Specific results computed for $m \leq 5000$ and generated graphs can be found at `https://www2.karlin.mff.cuni.cz/~raskam/research/quad/`.

Results in Chapters 2, 4, 5 are original results of the author which are currently submitted [Ra].

1. Basic definitions and facts

1.1 Quadratic fields

Throughout the work, $D \geq 2$ will denote a squarefree rational integer.
We will work with real quadratic fields $K = \mathbb{Q}(\sqrt{D}) = \{a + b\sqrt{D}; a, b \in \mathbb{Q}\}$.

An element $\alpha \in K$ is said to be *integral* (over $\mathbb{Z}$) if it is a root of a monic polynomial over $\mathbb{Z}$. All integral elements of K form *the ring of integers* denoted by $\mathcal{O}_K$ or simply $\mathcal{O}$. For quadratic fields, it is well known that the basis of $\mathcal{O}$ is $\{1, \omega_D\}$, where $\omega_D = \sqrt{D}$ if $D \equiv 2, 3 \pmod 4$ and $\omega_D = (1 + \sqrt{D})/2$ if $D \equiv 1 \pmod 4$.

An algebraic integer $\alpha = x + y\sqrt{D} \in \mathcal{O}$ is *totally positive* if $\alpha > 0$ and $\alpha' > 0$, where $\alpha' = x - y\sqrt{D}$ is the Galois conjugate of α. We denote by $\mathcal{O}^+$ the set of all totally positive algebraic integers.

1.2 Indecomposable elements

The totally positive integers $\mathcal{O}^+$ can be viewed as an additive semigroup. In Chapter 4, the notion of *indecomposable* elements in this semigroup will be useful. They are by definition such elements $\alpha \in \mathcal{O}^+$ that cannot be written as sum of two other elements $\alpha = \beta + \gamma$ and $\beta, \gamma \in \mathcal{O}^+$. It is clear that indecomposable elements generate this whole semigroup.

Indecomposable elements in quadratic cases are closely tied to the continued fractions. The continued fractions of quadratic integers, their recurrence relations and structure were studied by Perron [Pe]. The structure of indecomposable elements was later described by Dress and Scharlau [DS]. In the following paragraph, we state these well-known facts, adopting the notation used by [HK].

Denote $\omega_D = [u_0, \overline{u_1, \ldots, u_s}]$ the continued fraction of ω_D and p_i/q_i its convergents. The sequences (p_i) and (q_i) then satisfy the recurrence relation

$$X_{i+2} = u_{i+2}X_{i+1} + X_i \text{ for } i \geq -1 \tag{1.1}$$

with the initial conditions $q_{-1} = 0$, $p_{-1} = q_0 = 1$ and $p_0 = u_0$ [Pe, §1]. Further, denote $\alpha_i = p_i - q_i\omega'_D$ (where $\omega'_D = (1 - \sqrt{D})/2$ if $D \equiv 1 \pmod 4$ and $-\sqrt{D}$ otherwise), $\alpha_{i,r} = \alpha_i + r\alpha_{i+1}$ and let $\varepsilon > 1$ be the fundamental unit of $\mathcal{O}$. Then the following facts are true (see e.g. [DS]):

- The indecomposable elements in $\mathcal{O}^+$ are exactly $\alpha_{i,r}$ with odd $i \geq -1$ and $0 \leq r \leq u_{i+2} - 1$, together with their conjugates.
- The sequence (α_i) satisfies the recurrence relation (1.1).

- The equality $\alpha_{i,u_{i+2}} = \alpha_{i+2,0}$ holds.
- The fundamental unit satisfies $\varepsilon = \alpha_{s-1}$ and $\alpha_{i+s} = \varepsilon\alpha_i$ for all $i \geq -1$.
- For the smallest totally positive unit $\varepsilon^+ > 1$, we have $\varepsilon^+ = \varepsilon$ if s is even and $\varepsilon^+ = \varepsilon^2 = \alpha_{2s-1}$ if s is odd.

Example. Consider $D = 6$ with continued fraction $\sqrt{6} = [2, \overline{2, 4}]$, therefore $s = 2$. Using the recurrence relations above, we get the following values.

i	-1	0	1	2	3	4
p_i	1	2	5	22	49	218
q_i	0	1	2	9	20	89
α_i	1	$2+\sqrt{6}$	$5+2\sqrt{6}$	$22+9\sqrt{6}$	$49+20\sqrt{6}$	$218+89\sqrt{6}$

In this case, we get exactly two indecomposables for each odd i, since always $u_{i+2} = 2$. For $i = -1$ we get $\alpha_{-1,0} = 1$, $\alpha_{-1,1} = 3 + \sqrt{6}$, for $i = 1$ we have $\alpha_{1,0} = 5 + 2\sqrt{6}$, $\alpha_{1,1} = 27 + 11\sqrt{6}$, etc.

It can be seen that $\varepsilon = \alpha_1 = 5 + 2\sqrt{6}$ is indeed the smallest totally positive unit and, for example, $\varepsilon\alpha_2 = (5 + 2\sqrt{6})(22 + 9\sqrt{6}) = 218 + 89\sqrt{6} = \alpha_4$.

1.3 Quadratic forms

We define an *n-ary quadratic form* f over a ring R as a degree 2 homogeneous polynomial $f(x_1, \ldots, x_n) = \sum_{1\leq i\leq j\leq n} a_{ij}x_ix_j$ where $n \in \mathbb{Z}_{\geq 1}$, $a_{ij} \in R$.

A quadratic form f can be associated with uniquely determined symmetric matrix A such that $\mathbf{x}^T A\mathbf{x} = f$ for $\mathbf{x} = (x_1, \ldots, x_n)^T$. Specifically,

$$A = \begin{pmatrix} a_{11} & \frac{a_{12}}{2} & \cdots & \\ \frac{a_{12}}{2} & a_{22} & \cdots & \\ \vdots & & \ddots & \\ \frac{a_{1n}}{2} & & & a_{nn} \end{pmatrix}.$$

For binary quadratic form $f(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2$ we define its *determinant* D as $D = ac - \frac{b^2}{4}$.

We say that a quadratic form f represents a number N over R if there exist $x_1, \ldots, x_n \in R$ such that $f(x_1, \ldots, x_n) = N$.

We say that a quadratic form $f(x_1, \ldots, x_n)$ represents another quadratic form $g(y_1, \ldots, y_m)$ if there exists coefficients $t_{ij} \in R, 1 \leq i \leq n, 1 \leq j \leq m$ such that $f(\sum_{j=1}^m t_{1j}y_j, \ldots, \sum_{j=1}^m t_{nj}y_j) = g(y_1, \ldots, y_n)$. If we denote $T = (t_{ij}) \in R^{n\times m}$ and A, resp. B, is the matrix associated with f, resp. g, then this transformation can be written as $T^T AT = B$.

An easy consequence is that if f represents g and g represents some $x \in R$, then f represents x as well.

Example. The ternary quadratic form $x_1^2+x_2^2+3x_3^2$ represents the binary quadratic form $5y_1^2+4y_1y_2+7y_2^2$ through substitution $x_1 = y_1+2y_2$, $x_2 = 2y_1$ and $x_3 = y_2$. Using matrices, this can be written as

$$\begin{pmatrix} 1 & 2 & 0 \\ 2 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \\ 2 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 5 & 2 \\ 2 & 7 \end{pmatrix}.$$

Example. Another useful observation is that our problem of representation of elements by the sum of squares can be reformulated using quadratic forms. Since the Pythagoras number of quadratic rings of integers is at most 5 (the proof by Peters will be shown in Chapter 3), we are interested in which numbers are represented by the quadratic form $x_1^2+x_2^2+x_3^2+x_4^2+x_5^2$ over $\mathbb{Q}(\sqrt{D})$.

2. Bounds on m and D

If we look at all elements of the form $x + k\sqrt{D}$ for some fixed k, there exists minimal $x = 1 + \lfloor k\sqrt{D} \rfloor$ for which the element is still totally positive. As we are interested in sums of squares and $\sum(a_i + b_i\sqrt{D})^2 = \sum(a_i^2 + Db_i^2) + \sum 2a_ib_i\sqrt{D}$, it is therefore useful to study the minimum of $\sum a_i^2 + b_i^2 D$ for some fixed value of $\frac{k}{2} = \sum a_ib_i$. If this minimum is larger than $1 + \lfloor k\sqrt{D} \rfloor$, we obtain a totally positive element which can't be represented as the sum of squares.

These ideas will be properly formulated in the proofs later. We will also see that we can impose on a_i, b_i further restrictions that they are non-negative and sometimes congruent modulo 2. As can be seen in the following lemmata, this minimization question can be more easily answered if we know how large is D in comparison to m. To simplify our future formulations, it is convenient to introduce the following sets of intervals depending on m:

(a) $$I_t(m) = \begin{cases} \left[\frac{m^2}{t(t+1)}, \frac{m^2}{(t-1)t}\right] & \text{if } t > 1 \\ \left[\frac{m^2}{2}, \infty\right) & \text{if } t = 1 \end{cases}$$

(b) $$J_t(m) = \begin{cases} \left[\frac{m^2}{t(t+2)}, \frac{m^2}{(t-2)t}\right] & \text{if } t > 2 \\ \left[\frac{m^2}{t(t+2)}, \infty\right) & \text{if } t \in \{1, 2\} \end{cases}$$

Here, m and t are positive rational integers and we will use just I_t, J_t if the value of m is clear from the context. It should be also noted that $\bigcup_{t\geq 1} I_t(m) = \bigcup_{t\geq 1} J_{2t}(m) = \bigcup_{t\geq 1} J_{2t-1}(m) = (0, \infty)$ for arbitrary fixed m.

Lemma 3. *Let a_i, b_i, $1 \leq i \leq n$ be non-negative integers satisfying $\sum_{i=1}^n a_ib_i = m$ for a fixed positive integer m. Let D be a real number and t a positive integer such that $D \in I_t = I_t(m)$. Then*

$$\sum_{i=1}^n a_i^2 + Db_i^2 \geq \frac{m^2}{t} + tD.$$

Proof. Let $k = \sum b_i^2$. By Cauchy-Schwarz inequality

$$\sum a_i^2 \geq \frac{\left(\sum a_ib_i\right)^2}{\sum b_i^2} = \frac{m^2}{k}.$$

Now $\sum a_i^2 + Db_i^2 \geq \frac{m^2}{k} + kD$, so it is enough to prove $\frac{m^2}{k} + kD \geq \frac{m^2}{t} + tD$, which is equivalent to $(m^2 - tkD)(t - k) \geq 0$. This inequality holds by our assumption on D – since $Dt(t-1) \leq m^2 \leq Dt(t+1)$, both factors always have the same sign. □

In other words, the function $\frac{m^2}{x} + xD$ attains its minimum over positive integers at $x = t$. The value $2m\sqrt{D}$, the minimum of this function over positive reals, turns out to be too weak in the context of the following proofs.

For the case of equality, one only needs the equality in the Cauchy-Schwarz inequality (if and only if $a_i = rb_i$ for some fixed r) and $\sum b_i^2 = t$. Together they imply $rt = \sum rb_i^2 = \sum a_i b_i = m$, so $r = \frac{m}{t}$. Since $a_i = rb_i$ is integer, $t \mid b_i m$. Using $t \sum b_i^2 = t^2 \mid b_i^2 m^2$, we get that t must divide m^2 and it can be easily seen that this condition is also sufficient for the existence of suitable a_i, b_i. As an example, if m is divisible by t, the case of equality can be achieved for all D (one simply uses $a_i = \frac{m}{t}$, $b_i = 1$ for $i \leq t$).

We will also need a version of the previous lemma with an extra condition on the parity of a_i, b_i. Then the inequalities can be refined in the following way:

Lemma 4. *Let $a_i \equiv b_i \pmod 2$, $1 \leq i \leq n$ be non-negative integers satisfying $\sum_{i=1}^n a_i b_i = m$ for a fixed positive integer m. Let D be a real number and $t \equiv m \pmod 2$ a positive integer such that $D \in J_t = J_t(m)$. Then*

$$\sum_{i=1}^{n} a_i^2 + Db_i^2 \geq \frac{m^2}{t} + tD.$$

Proof. Let $k = \sum b_i^2$. The additional condition implies $m = \sum a_i b_i \equiv \sum b_i^2 = k \pmod 2$. In the same fashion as in the proof of the previous lemma, it is sufficient to look at the minimum of the function $f(x) = \frac{m^2}{x} + xD$ over positive integers congruent to m modulo 2. We already know the minimum over all positive integers is equal to $f(t)$ if and only if $D \in I_t$. If $t \equiv m \pmod 2$ we are almost done since $I_t \subset J_t$. In the case $t \not\equiv m \pmod 2$, the minimum of this function over positive integers congruent to m modulo 2 must be either $f(t-1)$ or $f(t+1)$ since this function has only one local minimum over positive reals. It can be easily seen that $f(t-1) \leq f(t+1)$ if and only if $D \geq \frac{m^2}{(t-1)(t+1)}$, which concludes the proof. □

Given the conditions of the first lemma, if $D \geq \frac{m^2}{2}$, then $\sum a_i^2 + Db_i^2 \geq m^2 + D$. If we add the parity condition, the minimum is $m^2 + D$ for $D \geq \frac{m^2}{3}$ and odd m, resp. $\frac{m^2}{2} + 2D$ for $D \geq \frac{m^2}{8}$ and even m. Even though we won't use these special cases explicitly, they will give rise to the general necessary bounds for D in terms of m.

Both of these lemmata can be utilized to greatly restrict possible values of D for which all elements of $m\mathcal{O}^+$ are represented as the sum of squares in $\mathcal{O}$. For fixed k, one could simply consider the smallest totally positive element α of the form $a + k\sqrt{D}$ and look when $m\alpha$ can be represented as the sum of squares. Combining these results for all possible k and I_t, J_t gives rise to the following proposition.

Proposition 5. *Let $K = \mathbb{Q}(\sqrt{D})$ with $D \geq 2$ squarefree and a positive integer m.*

(a) *If $D \equiv 2, 3 \pmod 4$, $t, k \in \mathbb{Z}_{>0}$, $D \geq m$ and*

$$\sqrt{D} \in \left[\frac{mk}{2t} + \frac{\sqrt{m}}{\sqrt{t}}, \frac{mk}{2(t-1)} - \frac{\sqrt{m}}{\sqrt{t-1}}\right],$$

then not *all elements of* $m\mathcal{O}^+$ *are represented as the sum of squares in* $\mathcal{O}$. *This interval is non-empty only for*

$$m \geq \frac{4t\,(t-1)\left(2t-1+2\sqrt{t(t-1)}\right)}{k^2}.$$

(b) *If* $D \equiv 1 \pmod 4$, $t, k \in \mathbb{Z}_{>0}$, $t \equiv mk \pmod 2$, $D \geq 4m$ *and*

$$\sqrt{D} \in \left[\frac{mk}{t} + \frac{2\sqrt{m}}{\sqrt{t}}, \frac{mk}{t-2} - \frac{2\sqrt{m}}{\sqrt{t-2}}\right],$$

then not *all elements of* $m\mathcal{O}^+$ *are represented as the sum of squares in* $\mathcal{O}$. *This interval is non-empty only for*

$$m \geq \frac{t\,(t-2)\left(2t-2+2\sqrt{t(t-2)}\right)}{k^2}.$$

For $t = 1$ *if* $D \equiv 2, 3 \pmod 4$, *resp.* $t \in \{1, 2\}$ *if* $D \equiv 1 \pmod 4$, *we define the right bound of the intervals to be* ∞ *and they are therefore always non-empty.*

Proof. Let's start with the case $D \equiv 2, 3 \pmod 4$.

For an arbitrary positive integer k, consider $\alpha = \left\lfloor k\sqrt{D}\right\rfloor + 1 + k\sqrt{D}$ and suppose $m\alpha = \sum(\alpha_i)^2$ for some $\alpha_i = a_i + \sqrt{D}b_i \in \mathcal{O}$. Without loss of generality, we can choose $a_i \geq 0$ for all i and $b_i \geq 0$ if $a_i = 0$. For the sake of contradiction, suppose there exists some i such that $b_i < 0$ and $a_i > 0$. We then have $m\alpha' \geq (\alpha_i')^2 = a_i^2 + b_i^2 D + 2a_i(-b_i)\sqrt{D} \geq 1 + D + 2\sqrt{D} \geq m$ for $D \geq m$, which is impossible because $\alpha' < 1$. Therefore, we can assume $b_i \geq 0$ for all i.

If we compare the irrational parts in the expression of $m\alpha$, we get $mk = 2\sum a_i b_i$. The choice of $k = 1$ immediately eliminates all odd m, so we can consider only even m. If we also compare the rational parts, we can apply Lemma 3 to get

$$mk\sqrt{D} + m > m(\left\lfloor k\sqrt{D}\right\rfloor + 1) = \sum a_i^2 + b_i^2 D \geq \frac{m^2k^2}{4t} + tD,$$

for $D \in I_t\left(\frac{mk}{2}\right)$. This is impossible if $\sqrt{D} \geq \frac{mk}{2t} + \frac{\sqrt{m}}{\sqrt{t}}$ or if $\sqrt{D} \leq \frac{mk}{2t} - \frac{\sqrt{m}}{\sqrt{t}}$. Combining these constraints for $D \in I_t\left(\frac{mk}{2}\right)$ and $D \in I_{t-1}\left(\frac{mk}{2}\right)$, we get that if

$$\sqrt{D} \in \left[\frac{mk}{2t} + \frac{\sqrt{m}}{\sqrt{t}}, \frac{mk}{2(t-1)} - \frac{\sqrt{m}}{\sqrt{t-1}}\right],$$

$m\alpha$ can not be represented as the sum of squares. For this interval to be non-empty, inequalities

$$\frac{mk}{2t} + \frac{\sqrt{m}}{\sqrt{t}} \leq \frac{mk}{2\sqrt{(t-1)t}} \leq \frac{mk}{2(t-1)} - \frac{\sqrt{m}}{\sqrt{t-1}}$$

must hold, which happens for $m \geq \frac{4t(t-1)\left(2t-1+2\sqrt{t(t-1)}\right)}{k^2}$. The above interval is not well-defined for $t = 1$, for which we immediately get the right bound to be ∞ just from considering a single inequality for $D \in I_1\left(\frac{mk}{2}\right)$.

Now let's look at the case $D \equiv 1 \pmod 4$.

This time $\alpha = \left\lfloor \frac{k\sqrt{D}-k}{2} \right\rfloor + 1 + \frac{k+k\sqrt{D}}{2}$ and again $m\alpha = \sum_i (\alpha_i)^2$. However, this time $\alpha_i = \frac{a_i}{2} + \frac{b_i\sqrt{D}}{2}$ with $a_i \equiv b_i \pmod 2$. We can again assume $a_i \geq 0$ and $b_i \geq 0$ since $\frac{1+D}{4} + \frac{\sqrt{D}}{2} > m$ for $D \geq 4m$. By comparing irrational parts, we get $\sum a_i b_i = mk$. Analogously, comparing rational parts and using Lemma 4, we get

$$\frac{mk\sqrt{D}}{2} + m > m\left(\left\lfloor \frac{k\sqrt{D}-k}{2} \right\rfloor + 1 + \frac{k}{2}\right) = \sum \frac{a_i^2 + b_i^2 D}{4} \geq \frac{m^2k^2}{4t} + \frac{tD}{4}$$

for $D \in J_t(mk)$, where $t \equiv m \pmod 2$. The rest of the proof is identical, except this time we obtain intervals

$$\left[\frac{mk}{t} + \frac{2\sqrt{m}}{\sqrt{t}}, \frac{mk}{t-2} - \frac{2\sqrt{m}}{\sqrt{t-2}}\right],$$

which are non-empty for $m \geq \frac{t(t-2)(2t-2+2\sqrt{t(t-2)}}{k^2}$. Again, cases $t = 1$ and $t = 2$ have to be considered separately. □

The proof of Proposition 5 has a similar structure as the one used by [KY] to prove that if $D > 4m^2$ for $D \equiv 2, 3 \pmod 4$, resp. $D > 16m^2$ for $D \equiv 1 \pmod 4$, then not all elements of $m\mathcal{O}^+$ are sums of squares. Proposition 5 shows that the bound is actually around $\frac{m^2}{4}$, resp m^2 (simply consider the proposition for $k = 1$ and t the lowest possible).

The benefit of Proposition 5 is that not only it gives better bounds, it also gives quite good insight into the structure of the problem and dependence of D on m. For example, if $D \equiv 2, 3 \pmod 4$, these solutions can be only "clustered" around values $m^2/4$, $m^2/16$, …, $m^2/4i^2$ and with increasing m, we get more accurate approximations for how large these clusters can be. The basic restrictions can be seen just by simply considering $k = 1$. An interesting follow-up question is what is the intersection of all these intervals for given m. As we will show in the next theorem, for parameters k, t with ratio $k : t$ close to a fixed value, these intervals can be typically grouped together to create one large interval between $m/2i$ and $m/2(i-1)$. This behaviour can be seen in Figure 2.1, containing computed data as well as these summarized bounds obtained by Theorem 2. It is important to note that there are only finitely many interesting intervals for fixed m – if k and t are large enough, then the interval is empty or it only affects $D \geq m^2$, for which we already know the conditions are not satisfied.

Theorem 2. *Let $K = \mathbb{Q}(\sqrt{D})$ with $D \geq 2$ squarefree and a positive integer m. If $\sqrt{D}$ lies in one of the following intervals, then* not *all elements of $m\mathcal{O}^+$ can be represented as the sum of squares:*

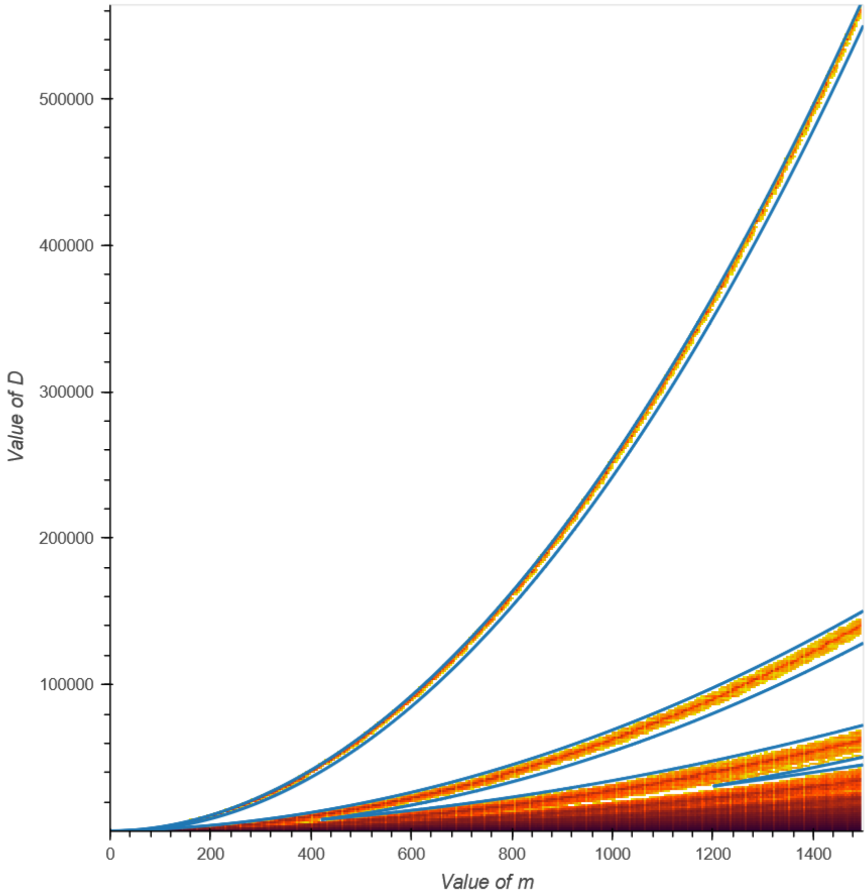

Figure 2.1: Case $D \equiv 2, 3 \pmod 4$. Red dots represent pairs (m, D) such that all elements of $m\mathcal{O}^+$ are sums of squares.

(a) $\left[\frac{m}{2} + 4, \infty\right)$, $\left[\frac{m}{2i} + i\sqrt{40}, \frac{m}{2(i-1)} - (i-1)\sqrt{70}\right]$ *for integer* $i > 1$ *and* $D \equiv 2, 3 \pmod 4$*,*

(b) $\left[\frac{m}{2} + 8, \infty\right)$, $\left[\frac{m}{2i} + 2i\sqrt{40}, \frac{m}{2(i-1)} - 2(i-1)\sqrt{70}\right]$ *for integer* $i > 1$*,* $D \equiv 1 \pmod 4$ *and even* m*,*

(c) $[m + 4, \infty)$, $\left[\frac{m}{2i+1} + (4i+2)\sqrt{40}, \frac{m}{2i-1} - (4i-2)\sqrt{70}\right]$ *for integer* $i > 0$*,* $D \equiv 1 \pmod 4$ *and odd* m*.*

Proof. We will prove only the case $D \equiv 2, 3 \pmod 4$, the other cases can be handled analogously.

By Proposition 5, we have intervals

$$S(t, k) = \left[\frac{mk}{2t} + \frac{\sqrt{m}}{\sqrt{t}}, \frac{mk}{2(t-1)} - \frac{\sqrt{m}}{\sqrt{t-1}}\right].$$

We want to look at these restrictions in intervals $\frac{m}{2i} \leq \sqrt{D} \leq \frac{m}{2(i-1)}$.

First, let's handle the case $i = 1$ when the upper bound of the interval is infinity and lower bound is around $\frac{m}{2}$. Intervals $S(t, k)$ are a part of this interval exactly when $k \geq t$, however, the cases $k > t$ are uninteresting since they are subintervals of some other intervals for smaller k. Therefore, we are only interested in intervals $S(t,t)$. The lower bounds of these intervals get lower with increasing t, so if we want to unite them without problems, we need to check there are no gaps between them – meaning the upper bound of $S(t+1,t+1)$ is larger than the lower bound of $S(t,t)$. This is equivalent to the inequality

$$\frac{mt}{2t} + \frac{\sqrt{m}}{\sqrt{t}} \leq \frac{m(t+1)}{2t} - \frac{\sqrt{m}}{\sqrt{t}},$$

which is true for $m \geq 16t$. Since we consider fixed value of m and t is integer we get a bound $t \leq \lfloor \frac{m}{16} \rfloor$. When the above inequality holds, the intervals are also all non-empty, so in total

$$\bigcup_{t=1}^{\lfloor \frac{m}{16} \rfloor + 1} S(t,t) = \left[\frac{m}{2} + \sqrt{\frac{m}{\lfloor \frac{m}{16} \rfloor + 1}}, \infty \right) \supset \left[\frac{m}{2} + 4, \infty \right).$$

In the case $i > 1$, interval $\frac{m}{2i} \leq \sqrt{D} \leq \frac{m}{2(i-1)}$ contains $S(t,k)$ for $k(i-1) < t \leq ki$, so there are exactly k intervals for fixed k. We are again interested only in the ones closest to the boundaries – $S(k(i-1)+1,k)$ and $S(ki,k)$ since the other ones lie between these two and are typically contained in some $S(t,k)$ for smaller k. We again need $S(k(i-1)+1,k) = S(t_1,k_1)$ and $S((k+1)(i-1)+1,k+1) = S(t_2,k_2)$ to intersect and the same for $S(ki,k)$ and $S((k+1)i,k+1)$. For the first pair to intersect it is sufficient if $m > t_2(i-1)^2 4(3+2\sqrt{2})$, which gives upper estimate $\frac{m}{2(i-1)} - (i-1)\sqrt{70}$. For the other pair, it can be estimated to be sufficient if $m > t_2 i^2 4(\frac{5}{2} + \sqrt{6})$, which gives lower estimate $\frac{m}{2i} + i\sqrt{40}$. Altogether, if $\sqrt{D}$ is in interval

$$\left[\frac{m}{2i} + i\sqrt{40}, \frac{m}{2(i-1)} - (i-1)\sqrt{70} \right],$$

then not all elements can be represented as sum of squares.

For completeness of the proof, it is easy to see by $AM - GM$ inequality that in any of these intervals $\sqrt{D} \geq \min(\frac{m}{2i} + i\sqrt{40}, \frac{m}{2} + 4) \geq 2\sqrt{2m}$, which complies to the necessary condition $D \geq m$ in Proposition 5. □

Again, it is important to note that for a fixed m, only finitely many of these intervals are non-empty. Constants $\sqrt{40}$ and $\sqrt{70}$ used in the previous theorem are deliberately inaccurate so the theorem can be stated for all m simultaneously. Asymptotically for $m \longrightarrow \infty$ these constants can be improved to 4 as for $D \equiv 2,3 \pmod 4$ the optimal t is around $16m \cdot i^2$.

To conclude this chapter, let's summarize all the known necessary and sufficient bounds for D in terms of m.

Corollary 6. *Let $K = \mathbb{Q}(\sqrt{D})$ with $D \geq 2$ squarefree.*

(a) *If $D \equiv 2,3 \pmod 4$ and $D \geq \left(\frac{m}{2} + 4\right)^2$, then* not *all elements of $m\mathcal{O}^+$ are represented as the sum of squares in $\mathcal{O}$.*

(b) *If* $D \equiv 1 \pmod 4$*, m is even and* $D \geq \left(\frac{m}{2}+8\right)^2$*, then* not *all elements of* $m\mathcal{O}^+$ *are represented as the sum of squares in* $\mathcal{O}$*.*

(c) *If* $D \equiv 1 \pmod 4$*, m is odd and* $D \geq (m+4)^2$*, then* not *all elements of* $m\mathcal{O}^+$ *are represented as the sum of squares in* $\mathcal{O}$*.*

(d) *If* $D \leq m$ *for* $D \equiv 2, 3 \pmod 4$ *and even m or if* $D \leq 2m$ *for* $D \equiv 1 \pmod 4$*, all elements of* $m\mathcal{O}^+$ *are represented as the sum of squares in* $\mathcal{O}$*.*

(e) *If m is odd and* $D \equiv 2, 3 \pmod 4$*, then* not *all elements of* $m\mathcal{O}^+$ *are represented as the sum of squares in* $\mathcal{O}$*.*

Proof. Parts $(a) - (c)$ are direct consequences of Theorem 2. Parts $(d), (e)$ has already been proven by [KY] in Theorem 1. Proof of the part (d) will be outlined in the next section, whilst the part (e) is a consequence of the comparison of irrational parts in the sum of squares, which can be seen in the proof of Proposition 5. □

In Chapter 4, we will look closely at some specific values of D to show that these restrictions are in some sense accurate.

3. Peters theorem

In this chapter, we will try to look at the other side of the problem, which is showing that for chosen D and m all elements of $m\mathcal{O}^+$ are represented as the sum of squares. The key element of the following work will be a result proved by Peters [Pet], which characterises when an element is the sum of squares. Since the proof in the original paper is written in German, we provide an English version for the benefit of the reader.

Theorem 7. [Pet, Satz 2] *Let $K = \mathbb{Q}(\sqrt{D})$ with $D > 0$ squarefree. Then $\alpha \in \mathcal{O}^+$ of the form*

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

is the sum of 5 squares if and only if there exist rational integer c, with additional condition $c \equiv b \pmod 2$ if $D \equiv 1 \pmod 4$, such that

$$c \in \begin{cases} \left[\frac{2a+b-2\sqrt{N(\alpha)}}{D}, \frac{2a+b+2\sqrt{N(\alpha)}}{D}\right] & \text{if } D \equiv 1 \pmod 4, \\ \left[\frac{a-\sqrt{N(\alpha)}}{2D}, \frac{a+\sqrt{N(\alpha)}}{2D}\right] & \text{if } D \equiv 2, 3 \pmod 4. \end{cases}$$

Before showing the proof, we will need the following technical lemma.

Lemma 8. *The quadratic form $x_1^2+x_2^2+x_3^2+x_4^2+x_5^2$ represents all binary quadratic forms $ay_1^2 + by_1y_2 + cy_2^2$ for $a, b, c \in \mathbb{Z}$, $a \geq 0$, $c \geq 0$ and $D = ac - b^2 \geq 0$.*

Sketch of the proof. This is not a full proof, since we do not define some of the used terms and notions.

The quadratic form $f = x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2$ is the only form in its genus. Therefore, by [OMe, 102:5], if we prove that the form $ay_1^2 + by_1y_2 + cy_2^2$ can be represented locally (over p-adic integers $\mathbb{Z}_p$ and $\mathbb{R}$), they it can also be represented globally (over $\mathbb{Z}$), which is what we want.

Assume $p \neq 2$. Then by [Jo, Theorem 32], our binary form $ay_1^2 + by_1y_2 + cy_2^2$ is (p-adically) equivalent to a diagonal form $g = ny_1^2 + my_2^2$, $n, m \in \mathbb{Z}_p$. By [Jo, Corollary 34a, 34b], the binary form $x_1^2 + x_2^2$ represents a squarefree integer $N \in \mathbb{Z}_p$ if and only if $p \nmid N$ or $p \mid N$ with $\left(\frac{-1}{p}\right) = 1$, and ternary form $x_1^2+x_2^2+x_3^2$ represents all N. Therefore, if $p \nmid n$ we can find z_i's and w_j's such that $z_1^2+z_2^2 = n$, $w_1^2 + w_2^2 + w_3^2 = m$, so that the following substitution proves that f represents g (and thus $ay_1^2 + by_1y_2 + cy_2^2$ as well)

$$\begin{pmatrix} z_1 & z_2 & 0 & 0 & 0 \\ 0 & 0 & w_1 & w_2 & w_3 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} z_1 & 0 \\ z_2 & 0 \\ 0 & w_1 \\ 0 & w_2 \\ 0 & w_3 \end{pmatrix} = \begin{pmatrix} n & 0 \\ 0 & m \end{pmatrix}.$$

If $p \nmid m$, similar representation can be constructed. In the case $p \mid n$ and $p \mid m$, we get that $z_1^2 + z_2^2 = n - 1$ is solvable over $\mathbb{Z}_p$. Further, at least one of the relations $p \nmid m - 1 - z_1^2$ and $p \nmid m - 1 - z_2^2$ holds. Then, for example in the first case, we get $m - 1 - z_2^2 = w_1^2 + w_2^2$ for some $w_1, w_2 \in \mathbb{Z}_p$ and f represents g using transformation matrix

$$\begin{pmatrix} z_1 & z_2 & 1 & 0 & 0 \\ 0 & 1 & -z_2 & w_2 & w_3 \end{pmatrix}.$$

The case $p = 2$ has to be handled separately. Theorems $9a$ and $9b$ from [Jo] (which basically show a correspondence between the solutions of $X^TAX = B$ in $\mathbb{Z}_p$ and the solutions of $X^TAX \equiv B \pmod{p^t}$ for matrices A, B and a sufficiently large t) in conjunction with the characterization of binary forms over $\mathbb{Z}_p$ can be used to show that all the binary forms above are indeed represented by $x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2$ in $\mathbb{Z}_2$.

Over $\mathbb{R}$, the representation is trivial [Jo, Theorem 6]. □

Proof of the Theorem 7. Consider $D \equiv 1 \pmod 4$ and $x \in \mathcal{O}_K^+$ of the form $x = x_1 + x_2\frac{1+\sqrt{D}}{2}$ and suppose $x = a + 2b\frac{1+\sqrt{D}}{2} + c\left(\frac{1+\sqrt{D}}{2}\right)^2$ for some $a, b, c \in \mathbb{Z}$. By comparing the coefficients, we get $x_1 = c\frac{D-1}{4} + a$ and $x_2 = 2b + c$. From there, it can be easily seen that for every choice of $c \equiv x_2 \pmod 2$, there exists exactly one pair of suitable (a, b).

One way to look at this is that x is represented by quadratic form $ay_1^2 + 2by_1y_2 + cy_2^2$ evaluated at $y_1 = 1$ and $y_2 = \frac{1+\sqrt{D}}{2}$. The determinant $D(c)$ of this form is equal to

$$D(c) = ac - b^2 = \left(x_1 - c\frac{D-1}{4}\right)c - \frac{(x_2 - c)^2}{4} = \frac{1}{4}\left(-Dc^2 + c(4x_1 + 2x_2) - x_2^2\right).$$

Viewing this as a quadratic function in c, this determinant is nonnegative if and only if $c \in \left[\frac{2x_1+x_2-2\sqrt{N(x)}}{D}, \frac{2x_1+x_2+2\sqrt{N(x)}}{D}\right]$, which is the interval from the theorem statement.

Therefore, if we assume that such a $c \equiv x_2 \pmod 2$ in this interval exists, we can accordingly find integers a, b and semipositive quadratic form $ay_1^2 + 2by_1y_2 + cy_2^2$ which represents x. By Lemma 8, this form is represented by $x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2$, therefore, x is represented by this form as well.

On the other hand, if we assume

$$x = \sum_{i=1}^{s} a_i \left(m_i + n_i\frac{1+\sqrt{D}}{2}\right)^2,$$

for some $a_i \geq 0$, $a_i, m_i, n_i \in \mathbb{Z}$, we get

$$x_1 = \sum_{i=1}^{s} a_i \left(m_i^2 + n_i^2\frac{D-1}{4}\right),$$

$$x_2 = \sum_{i=1}^{s} a_i \left(2m_i n_i + n_i^2\right).$$

For the choice $c = \sum_{i=1}^{s} a_i n_i^2 \equiv x_2 \pmod 2$,

$$4D(c) = \left(\sum_{i=1}^{s} a_i(2m_i + n_i)^2\right)\left(\sum_{i=1}^{s} a_i n_i^2\right) - \left(\sum_{i=1}^{s} a_i n_i(2m_i + n_i)\right)^2 \geq 0$$

by the Cauchy-Schwarz inequality. Therefore, this integer c also must be in the chosen interval.

In the case $D \equiv 2, 3 \pmod 4$, the situation can be handled analogously. Consider $x \in \mathcal{O}_K^+$ of the form $x = x_1 + 2x_2\sqrt{D} = a + 2b\sqrt{D} + c\left(\sqrt{D}\right)^2$. This time,

$$D(c) = ac - b^2 = (x_1 - cD)c - x_2^2 = -Dc^2 + cx_1 - x_2^2,$$

which is non-negative for $c \in \left[\frac{x_1 - \sqrt{N(x)}}{2D}, \frac{x_1 + \sqrt{N(x)}}{2D}\right]$.

For the other implications, given $x = \sum_{i=1}^{s} a_i \left(m_i + n_i\sqrt{D}\right)^2$, the choice $c = \sum_{i=1}^{s} a_i n_i^2$ provides the desired inequality

$$D(c) = (x_1 - cD)c - x_2^2 = \left(\sum_{i=1}^{s} a_i m_i^2\right)\left(\sum_{i=1}^{s} a_i n_i^2\right) - \left(\sum_{i=1}^{s} a_i m_i n_i\right)^2 \geq 0. \quad \square$$

Remark. Peters proved Theorem 7 not only for the quadratic form $x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2$ but also for quadratic forms $x_1^2 + x_2^2 + x_3^2 + x_4^2 + 2x_5^2$, $x_1^2 + x_2^2 + x_3^2 + x_4^2 + 3x_5^2$, $x_1^2 + x_2^2 + x_3^2 + 2x_4^2 + 2x_5^2$ and $x_1^2 + x_2^2 + x_3^2 + 2x_4^2 + 3x_5^2$. These forms satisfy the same local-global conditions needed in the proof of Lemma 8, which can be accordingly adjusted to handle all of these forms at the same time (in addition, the case $p = 3$ must be handled separately).

One direct consequence of this theorem is Corollary 6 (d). The norm of every element in $m\mathcal{O}^+$ is at least m^2; therefore, if m is large enough, the interval has the length of at least 1, resp. 2, so it must contain the desired integer.

Using the acquired necessary bounds and this theorem, we have a method for determining all D such that all elements of $m\mathcal{O}^+$ are represented as the sum of 5 squares. For example, for $m = 4$ we get

Theorem 9. *Let $K = \mathbb{Q}(\sqrt{D})$ with $D \geq 2$ squarefree. Then every element of $4\mathcal{O}^+$ is the sum of squares in $\mathcal{O}$ if and only if $D \in \{2, 3, 5, 6, 7, 10, 11, 13\}$.*

Proof. ”⇒” Assume all elements of $4\mathcal{O}^+$ can be represented as the sum of squares in $\mathcal{O}$.

At first, consider $D \equiv 2, 3 \pmod 4$. Using Proposition 5 for $t = 1$, $k = 1$, we get the bound $D < 16$. Furthermore, it can be easily verified that for $D \in$

$\{14, 15\}$, the element $4(\lfloor\sqrt{D}\rfloor+1+\sqrt{D})$ does not satisfy the condition in Theorem 7.

If $D \equiv 1 \pmod 4$, we obtain the bound $D \leq 23$ similarly. However, the values $D \in \{17, 21\}$ can be again excluded using the element $4\left(\left\lfloor \frac{1+\sqrt{D}}{2}\right\rfloor + \frac{1+\sqrt{D}}{2}\right)$.

"$\Leftarrow$" Consider $D \equiv 2, 3 \pmod 4$ and first, let's look at the general idea of the proof. Consider any element $\alpha = a + b\sqrt{D} \in \mathcal{O}^+$. Using Theorem 7, 4α is the sum of squares if and only if there exists a rational integer in the interval

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

If $4\sqrt{N(\alpha)} \geq D$, this is clearly true. It is, therefore, enough to consider only the elements of small norm (which can be, in general, done by solving finitely many generalized Pell equations).

(a) $D = 2, 3$. In this case, $4\sqrt{N(\alpha)} \geq D$ is always true.

(b) $D = 6$. In this case, the interval $\left[\frac{a-\sqrt{N(\alpha)}}{3}, \frac{a+\sqrt{N(\alpha)}}{3}\right]$ always contains an integer since $N(\alpha) \geq 1$.

(c) $D = 7$. It can be seen that the only potentially problematic case is $a \equiv \pm 2 \pmod 7$ (otherwise, $\frac{2a}{7}$ is at most $\frac{2}{7}$ away from the nearest integer). However, in that case, we get $N(\alpha) \equiv a^2 \equiv 4 \pmod D$ and $N(\alpha) \geq 4$ is indeed enough.

(d) $D = 10$. In this case, only $a \not\equiv \pm 1 \pmod 5$ and $N(\alpha) \leq 3$ would cause a problem. Analogously, $a \not\equiv \pm 1 \pmod 5$ implies $a^2 \equiv N(\alpha) \equiv -1 \pmod 5$, which results in $N(\alpha) \geq 4$.

(e) $D = 11$. In this case $a \equiv \pm 2 \pmod{11}$ causes a problem for $N(\alpha) \leq 3$, $a \equiv \pm 3$ for $N(\alpha) \leq 6$, $a \equiv \pm 4$ for $N(\alpha) \leq 2$. All these cases can be dealt with in the same fashion as above.

Consider $D \equiv 1 \pmod 4$, $\alpha = a + b\omega_D \in \mathcal{O}^+$. By Theorem 7, we need to prove there is an even integer in the interval

$$\left[\frac{4(2a+b) - 4\sqrt{4N(\alpha)}}{D}, \frac{4(2a+b) + 4\sqrt{4N(\alpha)}}{D}\right],$$

which is equivalent to the existence of an integer in the interval

$$\left[\frac{2(2a+b) - 2\sqrt{4N(\alpha)}}{D}, \frac{2(2a+b) + 2\sqrt{4N(\alpha)}}{D}\right],$$

For $D = 5$, this is clear. The only remaining case is $D = 13$.

Here, $4N(\alpha) = 4(a + \frac{b}{2})^2 - 4(\frac{b\sqrt{D}}{2})^2 = (2a+b)^2 - b^2 D \equiv (2a+b)^2 \pmod{D}$.

The only problematic residues are:

(a) $(2a+b) \equiv \pm 3 \pmod{13}$ and $4N(\alpha) \leq 8$ – not possible using the congruence above,

(b) $(2a+b) \equiv \pm 4 \pmod{13}$ and $4N(\alpha) \leq 6$ – not possible using the congruence above and the fact that $N(\alpha)$ is an integer.

□

In the second part of the proof, we dealt with the bad cases by clever manipulations with congruences and inequalities. This option might not be viable in the general case, but we can always solve corresponding Pell equations to get the elements of the given norm and get the desired congruences using their well-known structure and recurrence relations. On the other hand, if D does not meet the conditions, we will inevitably find a counterexample during this process.

Using this technique, one can verify the given statement for arbitrarily chosen $m\mathcal{O}^+$ and D. However, it gets progressively more tedious with increasing D and heavily relies on the ability to quickly solve the generalized Pell equation. In the next section, we will introduce an improved algorithm that uses indecomposable elements of $\mathcal{O}^+$ to avoid this issue.

4. The indecomposables

The characterization of indecomposable elements of $\mathcal{O}^+$ in quadratic fields can be used to show a few concrete results and also a general algorithm for solving the given problem.

The main idea is that instead of considering all elements of $\mathcal{O}^+$, we can just look at the indecomposables since if a and b can be both represented as the sum of squares, so can $a+b$. For D of a specific form, the indecomposables have such a nice structure that it can be used in combination with Theorem 7 to fully characterise which m satisfy the given statement. One easy consequence of the following theorems is that bounds in Corollary 6 are, in some sense, optimal.

Theorem 10. *Let $K = \mathbb{Q}(\sqrt{D})$ with squarefree $D = t^2 - 1$ for some even integer $t > 1$. For a positive rational integer m, the following are equivalent:*

(a) *All elements of $2m\mathcal{O}^+$ are represented as the sum of squares in $\mathcal{O}$.*

(b) *$m = (t-1)k + l$ for some $k \geq 0$ and $0 \leq l \leq 2k$.*

Proof. In all cases, $D \equiv 3 \pmod 4$. If we prove that for all indecomposable elements $\alpha \in \mathcal{O}^+$, $2m\alpha$ can be represented as sum of squares in $\mathcal{O}$, then obviously all elements of $2m\mathcal{O}^+$ can be represented.

The continued fraction representation of $\sqrt{t^2-1}$ is $[t-1, \overline{1, 2(t-1)}]$. For $i \geq -1$, define a sequence (α_i) by $\alpha_{-1} = 1$, $\alpha_0 = t - 1 + \sqrt{D}$, $\alpha_{i+2} = \alpha_{i+1} + \alpha_i$ for odd $i \geq -1$ and $\alpha_{i+2} = 2(t-1)\alpha_{i+1} + \alpha_i$ for even $i \geq 0$.
Using the facts mentioned in Section 1.2, all indecomposable elements in $\mathcal{O}^+$ are in this case α_i with odd $i \geq -1$, together with their conjugates. If α_i can be represented as the sum of squares, then its conjugate can be represented as well (just replace all the squared numbers by their conjugates), so we can consider only α_i.
It can be easily proven by induction that $\alpha_{2k+1} = \alpha_1^{k+1} = (t + \sqrt{t^2-1})^{k+1}$ either using the recurrence relations above or using facts from Section 1.2 ($\alpha_1 = \varepsilon$, $\alpha_{i+2} = \varepsilon\alpha_i$)

The important consequence it that $2m\alpha_{2k+1}$ can be represented as the sum of squares for all $k \geq -1$ if and only if $2m\alpha_1$ can be represented as the sum of squares. One implication is trivial and the other one comes from the following facts. If k is odd, then $\alpha_{2k+1} = \left(\alpha_1^{\frac{k+1}{2}}\right)^2$, so its is already a square in $\mathcal{O}$. If k is even $2m\alpha_{2k+1} = 2m\alpha_1 \cdot \alpha_{2k-1}$, both factors can be represented as the sum of squares in $\mathcal{O}$ so the product can be represented as well.

By Theorem 7, $2m\alpha_1 = 2m(t + \sqrt{t^2-1})$ can be represented as the sum of squares if and only if there is a rational integer in the interval

$$\left[\frac{2mt - \sqrt{N(2m\alpha_1)}}{2D}, \frac{2mt + \sqrt{N(2m\alpha_1)}}{2D}\right] = \left[\frac{m}{t+1}, \frac{m}{t-1}\right].$$

By substituing $m = (t-1)k + l$ for some integers $k \geq 0$, $0 \leq l < t-1$, it can be seen that this is true if and only if $l = 0$ or $\frac{m}{t+1} \leq k$, which is equivalent to $l \leq 2k$. □

The biggest m not satisfying the condition (b) is $m = (t-1)\frac{t-4}{2} + t - 2 = \frac{t^2-3t}{2}$, meaning that there exist infinitely many pairs $(D, m) = (t^2-1, \frac{t^2-3t}{2})$ such that not all elements of $2m\mathcal{O}^+$ are represented as the sum of squares. This shows the sufficient bound $D \leq \frac{m}{2}$ in Corollary 6(d) is quite precise.

On the other hand, the smallest non-zero m satisfying the condition is $m = t-1$, therefore all elements of $2m\mathcal{O}^+$ are represented as the sum of squares for $D = (m+1)^2 + 1$ (if this D is squarefree to be precise). This, again, shows that the necessary bound $D < (m+4)^2$ from Corollary 6(a) is somewhat accurate.

Theorem 11. *Let $K = \mathbb{Q}(\sqrt{D})$ with squarefree $D = (2t+1)^2 - 4$ for some integer $t > 1$. For positive rational integer m, all elements of $m\mathcal{O}^+$ are represented as the sum of squares in $\mathcal{O}$ if and only if m is one of the following form:*

(a) *$m = (4t-2)k + l$ for some $k \geq 0$ and $0 \leq l \leq 8k$ for l even,*

(b) *$m = (4t-2)k + l$ for some $k \geq 0$ and $0 \leq l \leq 8k - 2t - 3$ for l odd,*

(c) *$m = (4t-2)k + l$ for some $k \geq 0$ and $2t-1 \leq l \leq 8k + 2t + 3$ for l odd.*

Proof. The proof is quite similar to the proof of the previous theorem. This time, $D \equiv 1 \pmod 4$ and $\omega_D = \frac{1+\sqrt{D}}{2} = [t, \overline{1, 2t-1}]$ and again it holds that indecomposable elements are exactly powers of fundamental unit $\alpha_1 = t + \omega_D' = t + \frac{-1+\sqrt{D}}{2}$.

So it is equivalent to looking at when $m\alpha_1$ is the sum of squares, which, using Theorem 7, is exactly if and only if there is an integer $n \equiv m \pmod 2$ in the interval

$$\left[\frac{2mt + m - 2m}{D}, \frac{2mt + m + 2m}{D}\right] = \left[\frac{m}{2t+3}, \frac{m}{2t-1}\right].$$

Let $m = k(4t-2) + l$ for $k \geq 0$ and $4t - 2 > l \geq 0$. Then

$$\left[\frac{m}{2t+3}, \frac{m}{2t-1}\right] = \left[\frac{m}{2t+3}, 2k + \frac{l}{2t-1}\right].$$

If l is even, so is m, and the condition is satisfied if and only if $\frac{m}{2t+3} \leq 2k$, which is equivalent to $l \leq 8k$.

If l is odd and $l < 2t-1$, one needs $\frac{m}{2t+3} \leq 2k - 1$, equivalently $l \leq 8k - 2t - 3$. If $l \geq 2t-1$, only $\frac{m}{2t+3} \leq 2k + 1$ is needed, which is equivalent to $l \leq 8k + 2t + 3$.

One can see that $m = k(4t-2) + l$ with the discussed restrictions satisfy the interval condition even if we omit $l < 4t - 2$. This concludes the proof. □

The biggest even m and the biggest odd m not satisfying the conditions are both in the set $\{2t^2 - t - 2,\ 2t^2 - 3t - 1\}$. This, again, shows that the bound $D \leq 2m$ in 6(d) is quite sharp.

Regarding the smallest even m satisfying the conditions, we get $m = 4t - 2$, while the smallest odd m is $m = 2t - 1$. These arein close agreement with the necessary condition $D < (\frac{m}{2} + 8)^2$, resp. $D < (m + 4)^2$, from Corollary 6(b, c).

A similar approach could be naturally extended to other quadratic families, resulting in a system of (in)equalities that characterize all suitable m.

5. Algorithmic solution

The methods used in the previous chapter can be generalized to construct an algorithm that determines if all elements of $m\mathcal{O}^+$ are represented as the sum of squares. As was mentioned, one only needs to consider m-multiples of the indecomposables. If s is the period of the continued fraction of D, then $\varepsilon = \alpha_{s-1}$ is the fundamental unit and $\alpha_{i+s} = \varepsilon\alpha_i$. Therefore, there are only finitely many indecomposable elements (resp. their m-multiples) up to conjugation and multiplication by ε^2. If and only if all of them are represented, so are all elements of $m\mathcal{O}^+$. And we can easily check each of the elements using Theorem 7.

Unique indecomposable elements in $\mathcal{O}^+$ (uniqueness in the sense of the previous paragraph) are exactly $\alpha_{i,r}$ with odd $-1 \leq i \leq 2s-3$ and $0 \leq r \leq u_{i+2}-1$. Therefore, the number of unique indecomposables is $\sum_{i=1}^{s} u_{2i-1}$. Kala and Blomer [BK, Theorem 2] showed this sum to be $O(\sqrt{D}(\log(D))^2)$, which is therefore also the time complexity of this algorithm for single m and D.

Let's look at the time complexity for determining all D satisfying the conditions for fixed m. At first, consider only $D \equiv 2,3 \pmod 4$ and assume D satisfies the conditions. Necessary bounds in Theorem 2 imply $D < \left(\frac{m}{2}+4\right)^2$ and also $D \notin \left[\left(\frac{m}{2i}+i\sqrt{40}\right)^2, \left(\frac{m}{2(i-1)}-(i-1)\sqrt{70}\right)^2\right]$. We consider this interval only for finitely many i satisfying $\frac{m}{2i}+i\sqrt{40} < \frac{m}{2(i-1)}-(i-1)\sqrt{70}$ – the largest one being $i_{max} \asymp m^{\frac{1}{3}}$ (here notation $f \asymp g$ means $C|g(x)| < |f(x)| < D|g(x)|$ for some positive constants C, D and all sufficiently large x). Therefore, the smallest D excluded by the intervals is $D_{min} \asymp m^{\frac{4}{3}}$. As a consequece, if D satisfies the conditions, then either $D < D_{min}$ or D lies in one of the intervals $\left[\left(\frac{m}{2i}-i\sqrt{70}\right)^2, \left(\frac{m}{2i}+i\sqrt{40}\right)^2\right]$ for $i < i_{max}$. In the first case we can estimate the time complexity as $\sum_{D<D_{min}} O(\sqrt{D}(\log(D))^2) = O(m^{\frac{4}{3}} \cdot m^{\frac{4}{6}}(\log(m^{\frac{4}{3}}))^2) = O(m^2(\log(m))^2)$. In the second case, we have $O(m^{\frac{1}{3}})$ intervals and the length of each interval is $O(m)$. Therefore, the estimation of time complexity in the second case is

$$\sum_{i<i_{max}} O(m)\left(\frac{m}{2i}+i\sqrt{40}\right)\left(2\log(\frac{m}{2i}+i\sqrt{40})\right)^2 =$$

$$= O(m^2(\log(m))^2)\left(\sum_{i<i_{max}}\frac{1}{i}\right) + O(m(\log(m))^2)\left(\sum_{i<i_{max}} i\right) = O(m^2(\log(m))^3).$$

In the last equality we used $\sum_{i=1}^{n}\frac{1}{i} = O(\log(n))$ (see e.g. [Apo, Theorem 3.2]).

Overall, the time complexity for $D \equiv 2,3 \pmod 4$ is $O(m^2(\log(m))^3)$ and analogous argument can be made for $D \equiv 1 \pmod 4$. Hence, the time complexity of this algorithm (that for fixed m determines for which D all elements of $m\mathcal{O}^+$ can be represented as the sum of squares) is also $O(m^2(\log(m))^3)$.

The table below shows results for a few small m. The implementation in C++ (available at `https://github.com/raskama/number-theory/tree/main/quadr` atic) was used to obtain results for $m \leq 5000$. These data as well as generated graphs can be found at https://www2.karlin.mff.cuni.cz/~raskam/research/quad/.

m	D such that all elements of $m\mathcal{O}^+$ are sums of squares
1	5
2	2, 3, 5
3	5, 13, 17, 21
4	2, 3, 5, 6, 7, 10, 11, 13
5	5, 13, 17, 21, 29, 37
6	2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 21, 26, 29, 33
7	5, 13, 17, 21, 29, 33, 37, 41, 53, 61, 65, 77
8	2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 31, 37, 38, 53
9	5, 13, 17, 21, 29, 33, 37, 41, 53, 57, 61, 65, 69, 77, 85, 93, 101
10	2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 33, 34, 35, 37, 38, 41, 43, 53, 65, 85
11	5, 13, 17, 21, 29, 33, 37, 53, 57, 65, 73, 77, 85, 101, 145, 165

Bibliography

[Apo] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York (1976).

[BK] V. Blomer, V. Kala , *On the rank of universal quadratic forms over real quadratic fields*, Doc. Math. **23** (2018), 15–34.

[CP] H. Cohn, G. Pall, *Sums of four squares in a quadratic ring*, Trans. Amer. Math. Soc. **105** (1962), 536–556.

[DS] A. Dress, R. Scharlau, *Indecomposable totally positive numbers in real quadratic orders*, J. Number Theory **14**(3) (1982), 292-306.

[HK] T. Hejda, V. Kala, *Additive structure of totally positive quadratic integers*, 16 pp., Manuscripta Math. **163** (2020), 263-278.

[Jo] B. W. Jones, *The arithmetic theory of quadratic forms*, Mathematical Association of America (1950), 263-278.

[KRS] J. Krásenský, M. Raška, E. Sgallová, *Pythagoras numbers of orders in biquadratic fields*, arXiv:2105.08860.

[KT] V. Kala, M. Tinková, *Universal quadratic forms, small normes and traces over families of number fields*, arXiv:2005.12312.

[KY] V. Kala, P. Yatsyna, *Sums of squares in S-integers*, New York J. Math. **26** (2020), 1145 - 1154.

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

[OMe] O. T. O'Meara, *Introduction to quadratic forms*, Springer-Verlag, Berlin (1971).

[Pe] O. Perron, *Die Lehre von den Kettenbrüchen*, 1st edn, B. G. Teubner Verlag, Leipzig (1913).

[Pet] M. Peters, *Quadratische Formen über Zahlringen*, Acta Arith. **24** (1973), 157–164.

[Ra] M. Raška, *Representing multiples of m in real quadratic fields as sums of squares*, arXiv:2105.11423.

[Si1] C. L. Siegel, *Darstellung total positiver Zahlen durch Quadrate*, Math. Z. **11** (1921), 246-275.

[Si2] C. L. Siegel, *Sums of m-th powers of algebraic integers*, Ann. of Math. **46** (1945), 313–339.

[Ti] M. Tinková, *On the Pythagoras number of the simplest cubic fields*, arXiv:2101.11384.